



UNIVERSIDAD DE GRANADA
FACULTAD DE DERECHO
Programa de Doctorado en
Ciencias Jurídicas

COORDINADORA
Profa. Francisca Villalba
Pérez



**Università
degli Studi
di Ferrara**

DOTTORATO DI RICERCA IN
Diritto dell'Unione Europea e
ordinamenti nazionali
CICLO XXXIV

COORDINATORE
Prof. De Cristofaro Giovanni

Settore Scientifico Disciplinare:
Giurisprudenza

**THE EXTERNAL REACH OF THE INTEROPERABILITY OF LARGE-SCALE IT
SYSTEMS IN THE AFSJ**

Ph.D. student
Francesca Tassinari

Director
Prof. Teresa Fajardo
del Castillo

Director
Prof. Serena Forlati

Years 2019/2022



UNIVERSIDAD DE GRANADA

FACULTAD DE DERECHO

Departamento de Derecho internacional público y relaciones
internacionales

**THE EXTERNAL REACH OF THE INTEROPERABILITY OF LARGE-SCALE IT
SYSTEMS IN THE AFSJ**

Tesis doctoral presentada por
FRANCESCA TASSINARI

Las directoras:
Profa. Dra. Teresa Fajardo del Castillo

Profa. Dra. Serena Forlati

Programa de Doctorado en Ciencias Jurídicas
Granada, 2022



**Università
degli Studi
di Ferrara**

DOTTORATO DI RICERCA IN
Diritto dell'Unione Europea e ordinamenti nazionali

CICLO XXXIV

COORDINATORE Prof. De Cristofaro Giovanni

**THE EXTERNAL REACH OF THE INTEROPERABILITY OF LARGE-SCALE IT
SYSTEMS IN THE AFSJ**

Settore Scientifico Disciplinare: Giurisprudenza

Dottoranda

Dott.ssa Francesca
Tassinari

Tutore

Prof.ssa Teresa
Fajardo del Castillo

Tutore

Prof.ssa Serena Forlati

Anni 2019/2022

Editor: Universidad de Granada. Tesis Doctorales
Autor: Francesca Tassinari
ISBN: 978-84-1117-552-4
URI: <https://hdl.handle.net/10481/77708>

To my father, Bruno,
the only one who did not have the chance to
help me on this journey:
May his memory always guide my steps.

Table of contents

Acknowledgments	I
Abbreviations	III
Abstract	VII
INTRODUCTION	XI
INTRODUCCIÓN	XXVII
INTRODUZIONE	XLIII
CHAPTER I THE EUROPEAN UNION'S COMPETENCE ON THE PROTECTION OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA	1
1. Reinterpreting the human right to privacy in the digital age	4
1.1. The United Nations' delayed, soft response to technology challenges	4
1.2. The right to respect for private and family life and the Council of Europe's Convention 108 ..	11
2. The human right to privacy: Paving the way toward the establishment of a European Union's competence on the protection of personal data	25
2.1. The limits to the first internal market directive on the protection of personal data	31
2.2. A fundamental (human?) right to the protection of personal data	34
3. European Union's competence on the protection of personal data and on the free movement of such data	46
3.1. Article 16 of the Treaty on the Functioning of the European Union as a shared competence: Justifying subsidiarity, necessity, and proportionality in the light of the European Union's Charter of Fundamental Rights	46
3.2. Article 16 of the Treaty on the Functioning of the European Union as a horizontal but sectorial competence: The case of the Area of Freedom, Security and Justice	71
CHAPTER II THE EUROPEAN UNION'S EXTERNAL COMPETENCE ON PERSONAL DATA AND ITS TRANSFER TO THIRD COUNTRIES AND INTERNATIONAL ORGANISATIONS	107
1. Brief notes on the doctrine of implied external powers	110
1.1. The existence of implied European Union's external competences	112
1.2. The nature of implied European Union's external competences	114
2. The European Union's competence on the protection of personal data and on the free movement of such data: The existence and nature of the European Union's external action	123
2.1. The necessity of European Union's intervention to attain the objectives pursued by Article 16 of the Treaty on the Functioning of the European Union	129
2.2. The nature of the European Union's external competence in the field of personal data	157
3. The conclusion of "legally binding (enforceable) instruments"	171
3.1. Enforcement in public international law	173

3.2. Enforcement in the data protection field.....	184
4. The revision of existing international agreements.....	195
CHAPTER III THE EUROPEAN UNION'S LARGE-SCALE FREEDOM, SECURITY AND JUSTICE IT SYSTEMS	201
1. Large-scale IT systems enhancing inter-agency cooperation.....	204
2. Schengen Information System (SIS)	209
2.1. From the first to the second generation of the SIS	209
2.2. A “second” second generation of the SIS.....	229
3. European Asylum Dactyloscopy system (Eurodac)	240
3.1. The 2013 Eurodac recast Regulation.....	243
3.2. The 2016 Eurodac recast Proposal and its amendment	248
4. Visa Information System (VIS).....	253
4.1. The VIS Regulation	254
4.2. The access of law enforcement authorities and of Europol to the VIS: The VIS LEA Decision	265
4.3. The VIS revised Regulation.....	268
5. Entry-Exit System (EES).....	274
5.1. The 2008 Proposals on the EES and the Registered Traveller Programme.....	274
5.2. The 2017 Regulation on the establishment of the EES	280
6. European Travel Information and Authorisation System (ETIAS).....	290
7. European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN).....	301
CHAPTER IV THE INSTITUTIONALISATION OF THE EUROPEAN UNION'S COMPETENCE ON THE OPERATIONAL MANAGEMENT OF LARGE-SCALE IT SYSTEMS	311
1. Basic principles underpinning the delegation doctrine.....	313
1.1. The revised <i>Meroni</i> jurisprudence	317
1.2. The conclusion of administrative agreements and arrangements	322
2. The European Union Agency for the operational management of large-scale IT systems in the Area of Freedom, Security and Justice: eu-LISA	327
2.1. The progressive empowerment of eu-LISA	327
2.2. eu-LISA's structure and organisation	338
2.3. eu-LISA and the protection of personal data: The responsibility for the processing of personal data	346
3. The cooperation of eu-LISA domestically and internationally	355
3.1. The exchange of personal data with EU institutions, bodies, and offices	355
3.2. Any transfer of data to third countries and international organisations?	358

CHAPTER V THE INTEROPERABILITY OF LARGE-SCALE IT SYSTEMS IN THE AREA OF FREEDOM, SECURITY AND JUSTICE: CONTEXT, CONTENT AND PURPOSES	359
1. The interoperability of large-scale IT systems: Historical background	361
1.1. Interoperability in the aftermath of 11-S	365
1.2. The adoption of the interoperability package	368
2. The range of the interoperability Regulations	375
2.1. Interoperability in-between the Schengen <i>acquis</i> and the Area of Freedom, Security and Justice	377
2.2. A new IT infrastructure for large-scale IT systems: The components of interoperability	396
2.3. Interoperability's own objectives	412
2.4. Measures supporting interoperability	474
CHAPTER VI GLOBAL INTEROPERABILITY IN THE EUROPEAN UNION'S AREA OF FREEDOM, SECURITY AND JUSTICE	487
1. Global interoperability in the Area of Freedom, Security and Justice	490
1.1. The external dimension of large-scale IT systems	490
1.2. Interoperability with the Interpol's databases.....	518
2. The operational transfer of personal data from freedom, security and justice agencies to third countries and international organisations	537
2.1. Interoperability with the Europol's Information System.....	537
2.2. Eurojust's external relations	566
2.3. EBCG Agency's external relations.....	590
2.4. EUAA's external relations.....	622
CONCLUSIONS.....	637
CONCLUSIONES.....	661
CONCLUSIONI.....	685
Bibliography	709
Annex.....	892

Acknowledgments

It would be unfair for you to start reading this thesis without knowing that it is the fruit of not only my own perseverance, curiosity, and determination, but also the result of the suggestions, help, and support of a multitude of people I met during my pre-doctoral journey.

My first thanks go to my directors, Prof. Fajardo del Castillo and Prof. Forlati, who set me on the path of research believing in my abilities and stimulating my intellect. I would like to thank the Department of public international law and international relations of the University of Granada and the Department of international law of the University of Ferrara for welcoming me and giving unending input over the last three years. Special thanks go to Prof. Liñán Noguerras and Prof. Salerno for their work on European Union law and international law respectively.

Thanks to the European Commission, especially the Director General for Migration and Home Affairs, for having welcomed me to the B3 Unit, where I was able to add a more practical character to my work. A thank you also goes to the supervisor who monitored my period in Brussels, Mr Pérez Martínez, team leader of the interoperability group.

Under the direction of Prof. de Bruycker, the Odysseus summer school I attended during its XX edition was an indispensable forum where I could first present the results of my Ph.D. research. Prof. Vavoula has been a valuable source of input, some of which is reflected in the thesis. Also, Prof. Sartor's 2021 summer school on Artificial Intelligence and Law was an opportunity to reflect on the challenges new technologies bring to juridical science.

Among the prestigious scholars I met, Prof. Martín Rodríguez has certainly been one of the most patient and helpful in listening to both my doubts and thoughts. Also, my thanks go to Prof. Alberti, Prof. Annoni, Prof. Cancio Meliá, Prof. Lippi, Prof. Mercedes Moya, Prof. Portaceli Sevillano, Prof. Robles Carrillo, and Prof. Santos Vara for their insightful recommendations.

Of course, I should not forget all the friends and colleagues who helped me through my work. It would be impossible to name them all, but they should know that they have been a precious piece of the puzzle. Anyhow, I cannot but express my special thanks to my mother Catia, my sister Valentina, and my partner Diego. Finally, thanks to my little cat Nacho who stayed by my side, though sleeping, day and night.

Abbreviations

ABIS	Automated Biometric Information System
ADM	Automated Decision-Making
AFIS	Automated Fingerprints Identification System
AFSJ	Area of Freedom, Security and Justice
AI	Artificial Intelligence
API	Advance Passenger Information
Article 29 DPWP	Article 29 Data Protection Working Party
CCP	Common Commercial Policy
CEAS	Common European Asylum System
CEPOL	European Union Agencies for Law Enforcement Trainings
CFSP	Common Foreign and Security Policy
CIR	Common Identity Repository
CIS	Custom Information System
CJEU	Court of Justice of the European Union
CMS	Case Management System
COREPER	Committee of the Permanent Representatives of the Governments of the Member States to the European Union
COSI	Standing Committee on Operational Cooperation on Internal Security
CTC	Counter-Terrorism Coordinator
EBCG Agency	European Border Coast Guard Agency
ECHR	European Convention on Human Rights
ECOWAS	Economic Community of West African States
ECRIS	European Criminal Records Information System
ECRIS-TCN	European Criminal Records Information System for Third- Country Nationals
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EES	Entry Exit System
EIF	European Interoperability Framework
ENISA	European Union Agency for Cybersecurity

EPRIS	European Police Records Index System
ESMA	European Supervisory Authority
ESP	European Search Portal
ETIAS	European Travel Information and Authorisation System
EU	European Union
eu-LISA	European Union Agency for the operational management of large-scale IT systems in the Area of Freedom, Security and Justice
Eurodac	European Dactyloscopy system
Eurojust	European Union Agency for Criminal Justice Cooperation
Europol	European Union Agency for Law Enforcement
EUAA	European Union Asylum Agency
FNR	False Positive Rate
FPR	False Negative Rate
FTC	Failure to Capture
FTE	Failure to Enrol
FRA	European Union Fundamental Rights Agency
HLEG	High-Level Expert Group
ICD	Interface Control Document
ICRC	International Committee of the Red Cross
ICTs	Information and Communication Technologies
Interpol	International Criminal Police Organisation
IOM	International Organisation for Migration
IoT	Internet of Things
ISO	International Organisation for Standardisation
IT	Information Technology
JHA Area	Justice and Home Affairs Area
MID	Multiple Identity Detector
NUI	Interface of National Systems
OECD	Organisation for Economic Co-operation and Development
OLAF	European Anti-Fraud Office
PJCCM	Police and Judicial Cooperation in Criminal Matters
PNR	Passenger Name Record
QUEST	Querying Europol System

sBMS	shared Biometric Matching Service
SCH-EVAL	Schengen Evaluation
SIENA	Secure Information Exchange Network Application
SIRENE	Supplementary Information Request at the National Entries
SIS	Schengen Information System
SLTD	Stolen and Lost Travel Documents
TDAWN	Travel Documents Associated with Notices
TFTS	Terrorist Finance Tracking System
UNHCR	United Nations High Commissioner for Refugees
VIS	Visa Information System
WTO	World Trade Organisation

Abstract

Regulations (EU) 2019/817 and 2019/818 establish a framework for the interoperability between the European Union's information systems in the field of borders, visa, police and criminal judicial cooperation, asylum and migration. The dissertation analyses Article 50 regulating the communication of personal data to third countries and international organisations. It is assumed that the external dimension of the sister Regulations is layered on different degrees of interoperability that range from the interconnection of the Unions' components with the systems of various foreign parties, to the transfer of personal data performed by the staff of both national authorities and Union agencies to third countries and international organisations. The purpose of this work is to delimit the external reach of the interoperability Regulations by virtue of the principles and rules that regulate the European Union's external activity regarding the protection of personal data and on the free movement of such data.

Key words: European Union; Area of Freedom, Security and Justice; interoperability of large-scale IT systems; external reach; communication of personal data.

Résumé

Les Règlements (UE) 2019/817 et 2019/818 établissent un cadre pour l'interopérabilité entre les systèmes d'information de l'Union européenne dans le domaine des frontières, des visas, de la coopération policière et judiciaire criminelle, de l'asile et de la migration. La thèse analyse son article 50 qui régit la communication des données personnelles aux pays tiers et aux organisations internationales. Nous partons du principe que la dimension externe des Règlements frères repose sur différents degrés d'interopérabilité qui vont de l'interconnexion des éléments de l'Union avec les systèmes des parties étrangères, au transfert de données à caractère personnel effectué par les autorités nationales et le personnel des agences de l'Union vers des pays tiers et des organisations internationales. L'objectif est de délimiter la portée externe des Règlements d'interopérabilité en vertu des principes et des règles qui régissent l'activité externe de l'Union européenne en matière de protection des données personnelles et de libre circulation de ces données.

Mots clés: Union européenne; Espace de Liberté, Sécurité et Justice; interopérabilité des systèmes informatiques à grande échelle; portée externe; communication des données à caractère personnel.

Resumen

Los Reglamentos (UE) 2019/817 y 2019/818 establecen un marco para la interoperabilidad entre los sistemas de información de la Unión Europea en materia de fronteras, visados, cooperación policial y judicial penal, asilo y migración. La tesis analiza su artículo 50, que regula la comunicación de datos personales a terceros países y organizaciones internacionales. Se parte de la base de que la dimensión externa de los Reglamentos hermanos se asienta en diferentes grados de interoperabilidad que van desde la interconexión de los componentes de la Unión con los sistemas de terceras partes extranjeras, hasta la transferencia de datos personales realizada por las autoridades nacionales y el personal de las agencias de la Unión a terceros países y organizaciones internacionales. El objetivo es delimitar el ámbito de aplicación externo de los Reglamentos de interoperabilidad en virtud de los principios y normas que regulan la actividad exterior de la Unión Europea sobre la protección de datos personales y sobre la libre circulación de dichos datos.

Palabras clave: Unión Europea; Espacio de Libertad, Seguridad y Justicia; interoperabilidad de los sistemas de información de gran magnitud; alcance externo; comunicación de datos personales.

Riassunto

I Regolamenti (UE) 2019/817 e 2019/818 stabiliscono un quadro per l'interoperabilità tra i sistemi d'informazione dell'Unione Europea in materia di frontiere, visti, cooperazione di polizia e giudiziaria penale, asilo e migrazione. La tesi analizza il suo articolo 50 che regola la comunicazione dei dati personali a Paesi terzi e organizzazioni internazionali. S'ipotizza che la dimensione esterna dei Regolamenti fratelli sia organizzata su diversi gradi di interoperabilità che vanno dall'interconnessione delle componenti dell'Unione con i sistemi di parti terze straniere, al trasferimento dei dati personali effettuato dalle autorità nazionali e dal personale delle agenzie dell'Unione a Paesi terzi e organizzazioni internazionali. Lo scopo è quello di delimitare il campo di applicazione dei Regolamenti sull'interoperabilità in virtù dei principi e delle norme che regolano l'attività esterna dell'Unione Europea sulla protezione dei dati personali e sulla libera circolazione di tali dati.

Parole chiave: Unione europea; Spazio di Libertà, Sicurezza e Giustizia; interoperabilità dei sistemi IT su larga scala; portata esterna; comunicazione dei dati personali.

‘[...] We argue in favor of a new series of design principles to help us achieve optimal forms and levels of interoperability in the context of complex systems. Society needs interoperability, but systems must be designed to harness its benefits while minimizing its costs—and without going too far, without creating a system too complex to be managed. The stakes are extremely high’.

John Palfrey and Urs Gasser, *Interop: The promise and perils of highly interconnected systems*, 2012, p. 154.

INTRODUCTION

1. The “what” of the research

1.1. Background

In May 2019, the European Union (EU) adopted a framework regarding interoperability between its information technology (IT) systems in the field of borders, visa, police and criminal judicial cooperation, asylum, and migration. Regulations (EU) 2019/817¹ and 2019/818² (IO Regulations) aim at interconnecting the EU’s six large-scale IT systems that currently exist or are soon to be implemented within the Area of Freedom, Security and Justice (AFSJ) under the auspices of a new architecture that supports their functioning. These systems are: the Schengen Information System (SIS); the Visa Information System (VIS); the Entry-Exit System (EES); the European Travel Information and Authorisation System (ETIAS); the European Dactyloscopy system (Eurodac), and the System for the identification of Member States holding information on convicted third-country nationals and stateless persons (ECRIS-TCN). Interoperability is defined as the ability of systems to communicate, exchange data, and use the information previously stored in centralised, shared “databases”. Yet, the highly technical language used by the co-legislators has led to harsh criticism regarding its real reach which remains unclear until today.

Stretching across different legal systems, interoperability enables information and personal data³ to flow throughout different jurisdictions. According to Prof. Palfrey and Prof. Gasser:

‘One of the primary benefits of interoperability is that it can preserve key elements of diversity while ensuring that systems work together in the ways that matter most’⁴.

¹ Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, PE/30/2019/REV/1, OJL 135, 22.5.2019, pp. 27-84.

² Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, PE/31/2019/REV/1, OJL 135, 22.5.2019, pp. 85-135.

³ The current dissertation does not aim at tracing a frontline between the concept of “personal data” and that of “information” since, under the interoperability framework, person-related data – including those that serve to identify persons unequivocally – plays a protagonist role compared to the remaining information.

⁴ John Palfrey and Urs Gasser, *Interop: The Promise and Perils of Highly Interconnected Systems*, US, Basic Books, 2012, p. 11.

In 2012⁵, Bruening advanced the idea that ‘interoperability’ could also ensure the flow of information where different cultural approaches to privacy are in place⁶. According to the author, any solution to the issue of conflicting cultural backgrounds should have respected the existence of diverging concepts of privacy in national and regional regimes. In these terms, ‘legal interoperability’ is presented as an alternative to normative harmonisation, enabling the ‘compatibility’ of different legal systems, without the need to encounter domestic legislation. Specifically, Bruening maintains that interoperability should be supported by three cumulative features:

1. common principles;
2. accountability, and
3. cooperation between regulators.

In parallel, the White House specified⁷ that “global” interoperability should be based not on shared human rights values, but on the principals of mutual recognition and enforcement cooperation: the former is founded on the assumption that other legal systems comply with ‘common values surrounding privacy and personal data protection’⁸; the latter requires the organisation responsible for the processing activity to demonstrate its accountability.

However, in the EU context, transferring personal data without counting on harmonised normative standards risks undermining the guarantees set forth under Union legislation on the protection of personal data, which ordinarily requires a third country or international organisation to apply a level of protection “equivalent” to that of the EU. The human right to “privacy”, in its multifaceted conceptualisations, and the fundamental right to the

⁵ Paula J. Bruening, “Interoperability: analysing the current trends & developments”, *Data protection law & policy*, 2012, pp. 12-14.

⁶ Similarly, Amedeo Santusuosso and Alessandra Malerba, “Legal Interoperability as a Comprehensive Concept in Transnational Law”, *Law, Innovation and Technology*, Vol. 6 No. 51, 2014, pp. 51-73, p. 68, maintain: ‘[...] legal interoperability is able to explain some legal phenomena that are very different in kind and to encompass them in a unique conceptual frame’. This implies that differently from comparative disciplines that aim at uniformity, legal interoperability wants to: focus on differences rather than on similarities; put in contact (and make operative) elements that naturally would be separated because of some conceptual or linguistic misalignment, and offer a vision of more than two legal particles/systems working together.

⁷ The White House, *Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy*, Washington D.C., 2012, p. 31 ff.

⁸ Torben Holvad, “Mutual recognition, standards and interoperability”, in Matthias Finger and Pierre Messulam, *Rail economics, regulation and policy in Europe*, Cheltenham, Edward Elgar Publishing, 2015, pp. 275-302, p. 280:

‘The principle of mutual recognition is fundamental to the functioning of the EU Single Market and the free movement of goods within the European Union. It establishes that: Member States must allow a product that has been lawfully produced and marketed in another Member State into their own market. This is the case even if the product does not comply with the technical rules in that country. The mutual recognition principle can only be disregarded by a Member State in case of overriding general interest, such as that relating to public health or environmental protection [...]’.

protection of personal data firstly consecrated in Article 8 of the Charter of Fundamental Rights of the EU⁹ (CFREU), could be undermined when the disclosure of information regarding the individual leads to disproportionate interferences. After the Snowden scandal¹⁰ legal systems previously considered to be “close” to the European model have been regarded with mistrust as they have proved to be incompatible with the EU hierarchy of values. Consequently, within the EU legal order, “global interoperability” should be carefully balanced against individuals’ rights.

According to Article 50 of the sister Regulations, the communication of personal data to third countries, international organisations and private parties is regulated by the underlying large-scale IT systems and Union agencies’ regimes on the transfer of personal data. In addition, the IO Regulations advance a forthcoming Cooperation Agreement with the International Criminal Police Organisation (Interpol) which would interconnect interoperability with the Interpol databases of Stolen and Lost Travel Documents (SLTD) and of Travel Documents Associated with Notices (TDAWN). According to this norm:

‘Without prejudice to Article 31 of Regulation (EC) No 767/2008, Articles 25 and 26 of Regulation (EU) 2016/794, Article 41 of Regulation (EU) 2017/2226, Article 65 of Regulation (EU) 2018/1240 and the querying of Interpol databases through the ESP in accordance with Article 9(5) of this Regulation which comply with the provisions of Chapter V of Regulation (EU) 2018/1725 and Chapter V of Regulation (EU) 2016/679, personal data stored in, processed or accessed by the interoperability components shall not be transferred or made available to any third country, to any international organisation or to any private party’.

The co-legislators have presented the interoperability framework as an efficient and effective solution to manage the objectives of the AFSJ. Indeed, the rules underlying the communication of personal data echo those established by the EU in its data protection *acquis*, namely: Chapter V of the Data Protection Regulation for the European Union institutions, bodies, offices, and agencies (EUDPR)¹¹; Chapter V of the General Data Protection Regulation¹² (GDPR), and (eventually) Chapter V of the Law Enforcement

⁹ Charter of Fundamental Rights of the European Union, *OJ C* 326, 26.10.2012, pp. 391-407.

¹⁰ Edward Snowden translated by Esther Cruz Santaella, *Vigilancia Permanente*, Barcelona, Planeta, 2019.

¹¹ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.), *PE/31/2018/REV/1*, *OJ L* 295, 21.11.2018, pp. 39-98.

¹² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), *OJ L* 119, 4.5.2016, pp. 1-88.

Directive¹³ (LED). However, it is not clear whether, and in which terms, the external dimension of interoperability manages to respect the normative parameters set forth in international and EU law: Are the rules and principles applied by the EU to the communication of personal data to third parties in its external relations being respected, circumvented, or breached by interoperability?

1.2. Objective and research questions

1.2.1. Main objectives and underlying research question

The main purpose pursued by the current research is to determine the external reach of the interoperability framework established under Regulations (EU) 2019/817 and 2019/818, that is, their extent beyond the EU's external borders. Thus, this dissertation seeks to analyse whether the interoperability with foreign databases of Union centralised systems and components is lawful and “sustainable” – i.e., consistent¹⁴ – *vis-à-vis* the rules and principles underpinning the EU external action. Specifically, we will assess whether Article 50 of the IO Regulations complies with the international and supranational legal frameworks and, if so, whether the individuals' rights, especially the fundamental right to the protection of personal data, are truly guaranteed.

1.2.2. Ancillary questions

To answer the principal research question, the following sub-questions need to be addressed beforehand:

1. What does the EU's data protection *acquis* consist of and how it is shaped within the AFSJ?
2. How is the protection and transfer of personal data regulated in the EU?
3. How and for what purposes do large-scale IT systems process personal data?

¹³ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L* 119, 4.5.2016, pp. 89-131.

¹⁴ According to Article 7 of the Consolidated version of the Treaty on the Functioning of the European Union, *OJ C* 326, 26.10.2012, pp. 47-390 (TFEU): ‘The Union shall ensure consistency between its policies and activities, taking all of its objectives into account and in accordance with the principle of conferral of powers’.

4. What role does the European Union Agency for the operational management of large-scale IT systems in the Area of Freedom, Security and Justice (eu-LISA) actually play?
5. Apart from the interconnection of existing large-scale IT systems, what are the true colours – i.e., circumstances, objectives, and content – of the interoperability framework?
6. How does interoperability relate to the EU's external competence on the protection of personal data and on the free movement of such data?

1.3. Hypothesis

To answer our main research question, we expect that the external reach of interoperability takes on different shades. First of all, we believe that interoperability's external dimension should not be reduced to a mere support function for the underlying large-scale IT systems and Union agencies and that – apart from the interconnection with Interpol's databases, which is expressly foreseen – Article 50 of the IO Regulations establishes new means and channels for communicating personal data to third parties. Otherwise, such a norm would not bring any added value with respect to the rules on the transfer of personal data set forth for the underlying large-scale IT systems. As such, we advance the hypothesis that Article 50 of the IO Regulations would enable the interoperability of third countries and international organisations' databases with the Union's components to enhance the Union's operational capacity in the AFSJ, both in its internal and external dimensions. Such a hypothesis requires the analysis of the internal scope of interoperability as well as its added value with respect to the objectives pursued by the underlying large-scale IT systems.

On this basis we advance a second research hypothesis for which different degrees of interoperability could be envisaged in terms of direct interconnection and of data legibility. This thesis must be supported by the adoption of a broad definition of “transfer of personal data” including several types of tools that make the data available to other parties – e.g., the ‘exchange of personal data’ or the ‘disclosure of personal data’ – and should consider the peculiarities stemming from the data protection regime applicable within the AFSJ. Accordingly, our analysis does not embrace a literal, but a systematic interpretation of Article 50. By taking into account the techno-political evolution of large-scale IT systems in the past twenty years, we should appreciate that the agencies of the AFSJ with access to the interoperability architecture – namely, the European Union Agency for Law Enforcement

(Europol), the European Union Agency for Criminal Justice Cooperation (Eurojust), the European Border and Coast Guard Agency (EBCG Agency), and the European Union Asylum Agency (EUAA) – could access the centrally stored data and share it by virtue of administrative agreements and arrangements concluded between them and with third countries and international organisations.

Our premise suggests that the lawfulness and sustainability of any type of interoperability should be deductively evaluated on a case-by-case basis in light of the principles and rules that govern the EU external action in the field of personal data. The communication of personal data, whether performed by machines or human beings, must respect the legal framework regulating the EU – or its bodies’ – external activity, including the CFREU, to which it is subjected. These guarantees should not be circumvented for the sake of improved order and security within the AFSJ. Provided that the interoperability framework is expected to pose a heavier burden on third-country nationals than on Union citizens, appropriate safeguards would be needed to account for their vulnerable situation and, specifically, to prevent any discriminatory treatment, restriction or illegal repression of their rights. We believe that, in practice, the protection of some groups of people – e.g., children and asylum seekers – would be affected.

At this point, our research would be satisfactory, but not complete: We need to contemplate the possibility that the EU normative framework regulating the protection of personal data and the free movement of such data could be improved in order to overcome any lack of protection and legislative gaps. Assessing whether interoperability’s Article 50 conforms to the EU *acquis* might not be sufficient and *de lege ferenda* proposals must be made if we consider that Article 50 is expected to balance the need to cooperate with third parties to achieve freedom, security, and justice purposes with the transborder protection of fundamental rights.

2. The “why” of the research

Since the end of the ‘90s, evolution within the IT sector has been transforming the international community into a globalised, interconnected world. The spread and improvement of computing technology and Artificial Intelligence (AI), which lead the revolution as a result of the flood of information we disseminate every day¹⁵, are rising

¹⁵ Joint Research Centre Technical Report, *AI Watch: Beyond pilots: sustainable implementation of AI in public services*, Luxembourg, 2021, p. 32 ff.: ‘One of the most fundamental requirements of AI is data. By definition, AI relies on access being ensured to the “right” kind of data on which to perform its analyses, and which in most cases is augmented by the results of the analyses themselves. For many Public Sector organizations

concerns regarding the protection of individuals' human rights. As the European Data Protection Supervisor (EDPS) points out, information and communication technologies (ICTs) bring new challenges to the individuals' private sphere since personal data are processed in different forms – collected, sorted, filtered, transferred, or otherwise retained – which multiplies the risk of interferences¹⁶.

The IO Regulations are among the most recent reforms undertaken by the Union to efficiently safeguard its freedom of movement area, and are a response to the numerous crises it has faced. The urgency of the continuous threats to Schengen led to the introduction of interoperability before the launch of the EU Digital Strategy by Commissioner Von Der Leyen on 9 March 2021¹⁷. We therefore wonder whether such a potentially intrusive reform has been adopted with sufficient caution and awareness, or whether the co-legislators have, let us say, used the humanitarian crisis to promote a legal framework that restricts individuals' – especially, migrants' – fundamental rights.

The resolution of “old problems” with innovative tools triggers new research projects that scrutinise whether the new digital environment is provided with adequate guarantees to protect individuals' rights. After 11-S, the United States' (US) “collect it all” data storage programs showed that cyber-surveillance could disproportionately restrict the individuals' rights to privacy and, at supranational level, their right to the protection of personal data under the pretext of countering criminals and terrorists. From that moment on, a climate of mistrust towards intelligence services has been spreading around the world, hampering the transborder flow of data, which became a highly sensitive topic. The fact that the new interoperability framework set forth under Regulations (EU) 2019/817 and 2019/818 enables personal data to flow toward and from third parties, including legal orders applying different systems of human rights protection, questions the validity and consistency of unrestricted

though, fulfilling this requirement is a challenge, due to **a variety of obstacles in obtaining data of the quality and format they require**'. The Preliminary Opinion of the EDPS, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, Brussels, 10.03.2014, p. 9, reports that every day, 2.3 trillion gigabytes of data are collected and combined to generate services and global mapping.

¹⁶ See: the Opinion of the EDPS on *Promoting Trust in the Information Society by Fostering Data Protection and Privacy*, Brussels, 18.03.2010; the Executive summary of the Opinion of the European Data Protection Supervisor on the Communication from the Commission on 'The Digital Agenda for Europe — Driving European growth digitally', *OJ C* 358/17, 7.12.2013, and the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" {SEC(2009) 399} {SEC(2009) 400}, COM(2009) 0149 final, COM(2009) 149 final, Brussels, 30.3.2009.

¹⁷ The strategy is available at the official webpage of the European Commission at the following link www.ec.europa.eu. Note that 'a Europe fit for the digital age' is one of the key policy objectives agreed in the Joint Declaration of the European Parliament, the Council of the European Union and the European Commission, *EU Legislative Priorities for 2022*, Brussels, 2022.

“global interoperability”. Moreover, other non-derogative principles – e.g., the prohibition on discrimination and the *non-refoulement* – becomes relevant as soon as vulnerable groups of third country nationals are involved.

2.1. Previous studies

Provided that a first attempt to establish a framework for interoperability within the AFSJ dates back to the aftermath of 11-S, different studies correlated to our research topic have been carried out since the 2000s. In practice, two cultural waves could be recognised:

- a first batch of studies focuses on the interoperability between the SIS, the VIS, and the Eurodac, though this project was discarded because of legal, political, and technical concerns;
- a second batch of works emerged following the Communication of the European Commission on Stronger and Smarter Information Systems for Borders and Security adopted on 6 April 2016¹⁸ and concerns the IO Regulations or, more generally, large-scale IT systems.

In both cases, the Belgian school, headed by Prof. De Hert, has been a pioneer in advancing interoperability studies within the AFSJ, and it was later joined by other schools, including, the French school of Prof. Bigo, the Dutch school of Prof. Brouwer and, more recently, the London school of Prof. Vavoula. The latter is expected to publish an important monograph on large-scale IT systems shortly after the submission of this thesis.

2.2. Current situation

All contributions to the interoperability framework established by Regulations (EU) 2019/817 and 2019/818 adopt a single, internal normative approach: one that considers human rights. First of all, interoperability and its large-scale IT systems are analysed *vis-à-vis* the protection of individuals’ right to privacy and, even more importantly, *vis-à-vis* the fundamental right to the protection of personal data consecrated in the CFREU. Other studies assess the impact of the sister Regulations on the individual by taking into account that their personal data might be processed by Union agencies instead of national authorities. These contributions bring only partial results regarding the interoperability framework and, in some cases, lead to errors because of the lack of a holistic inspection. In sum, interoperability has been scrutinised from a specific disciplinary angle and we cannot count on a fully developed

¹⁸ Communication of the European Commission on Stronger and Smarter Information Systems for Borders and Security adopted on 6 April 2016, COM(2016) 205 final, Brussels, 6.4.2016.

theory on the external reach of Regulations (EU) 2019/817 and 2019/818. All in all, these studies remain extremely valuable: they acknowledge that different theories are applicable to the interoperability framework and that several theories must be taken into account when scrutinising its external reach. The resulting legal framework, though complex, makes our work as original as possible.

3. The “how” of the research

3.1. Legal framework

The foundation of this dissertation rests upon liberalism and humanism in the context of a targeted international organisation – i.e., the EU – based on the respect of human rights, individual freedoms, diversity, solidarity, and democracy¹⁹. As Prof. Liñán Nogueras affirms, the EU enjoys a derived legal personality, conditioned by the will of its Member States, and limited in its scope and content, which are determined by its functions²⁰. The configuration of a supranational legal order, moving toward the tightest possible integration of its Member States, enabled the development of a legal framework ensuring a ‘high level of protection’ to personal data, and for the purposes of Police and Judicial Cooperation in Criminal Matters (PJCCM), with unprecedented results. The EU digital leadership is sealed in a new competence that was conferred on the Union in 2007 in order to regulate the protection of personal data and the free movement of such data, namely Article 16 of the TFEU. The new competence builds a bridge between the fundamental right to the protection of personal data and to a private life outlined in Articles 8 and 7 of the CFREU, which became binding in 2009.

However, the guiding thread of our research is found not only in the EU internal *acquis* based on Article 16(2) TFEU, but also on the principles and rules the EU must respect as a global player subject to public international law when acting externally²¹. Consequently, the external reach of the IO Regulations must be analysed under a competence approach in the light of the regime on the transfer of personal data set forth in the GDPR, the LED, and the

¹⁹ Article 2 of the Consolidated version of the Treaty on European Union, *OJ C* 326, 26.10.2012, pp. 13-390 (TEU).

²⁰ See Diego Javier Liñán Nogueras, “La acción de la Unión: las relaciones exteriores (I)”, in Araceli Mangas Martín and Diego Javier Liñán Nogueras, *Instituciones y Derecho de la Unión Europea*, Madrid, Tecnos, 2020, on-line resource.

²¹ Conversely, our research does not take care of the cybersecurity international and supranational frameworks since the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, signed in Strasbourg on 12 May 2022, and the EU strategy on cybercrime were under revision.

EUDPR. Specifically, we should refer to the theories on the external relations of international organisations including the one concerning the EU. By virtue of the *AETR/ERTA*²² jurisprudence of the Court of Justice of the EU (CJEU), the Union could acquire an external (implied) competence to ensure that continental standards are not circumvented in cases where personal data is transferred to foreign authorities. The EU was the first player to adopt an “adequacy” or “geographical-based” model that empowers the European Commission to assess third parties’ legislations *vis-à-vis* that of the EU. According to this regime, the adoption of a decision on adequacy should be preferred to the conclusion of an international treaty or derogation clauses. In *Opinion 1/15*²³, the CJEU posited that the transfer of personal data, known as a Passenger Name Record (PNR), to a third country should be sealed in an international agreement framed under both Articles 87(2)(a) and 16(2) of the TFEU, covering measures concerning the transfer of personal data and the protection of such data, respectively. Assuming that the set of rules regarding the protection of personal data and its transfer might constitute an exercise of the EU’s competence on the protection of personal data and on the free movement of such data based on Article 16(2) of the TFEU will help clarify the adequacy decision/international agreements dichotomy.

Notably, this legal framework applies both when the Union acts directly and when it delegates the execution of its competences to external organisations and internal bodies. Provided that the second layer of the interoperability’s external dimension would be structured on the basis of those Union agencies that have access to the new IT infrastructure, a second main theory guides our research, that is, that of delegation. Specifically, the revisited *Meroni* judgment²⁴ complements the theory on implied external competences when Union agencies are delegated the conclusion of administrative agreements and arrangements since in the accomplishment of internal objectives cooperation with foreign authorities is required. The theory on EU external relations is based on the paramount principle of conferral imposing on the EU, as well as on its institutions, the duty to act within the limits established by the founding Treaties – that is, the explicit legal basis set down in the founding Treaties that confers upon the EU the power to act externally or, in the absence of an express provision, its empowerment via the theory of implied competences²⁵. Rather, the revised

²² C-22/70, *Commission of the European Communities v Council of the European Communities*. *European Agreement on Road Transport*, 31 March 1971, EU:C:1971:32.

²³ *Opinion 1/15*, 26 July 2017, EU:C:2017:592.

²⁴ C-9/56, *Meroni & Co., Industrie Metallurgiche, SpA v High Authority of the European Coal and Steel Community*, 13 June 1958, EU:C:1958:7.

²⁵ Jacopo Alberti, *Le Agenzie dell’Unione Europea*, Milano, Giuffrè, 2018, p. 33 ff., p. 419: ‘[...] agencies whose founding regulations do not provide for competence to act at international level are not always exempt from doing so [...]’ (our own translation).

Meroni doctrine gives the so-called “principal” authority²⁶ the ability to “shift its responsibility” to the delegated body and to actually delegate its competences. The external action of Union agencies is limited to so-called “technical-administrative” agreements or arrangements, being that their implementation is concluded in line with Article 218 TFEU or generally under EU legislation. As Advocate General Tesauro recalled:

‘[...] there are certain arrangements brought into being by specific administrative entities with a view to establishing forms of cooperation with the authorities of other States having similar powers. That category of "agreements", which are evidently not international agreements, concluded ° admittedly ° also by bodies lacking power to bind the State effectively at international level, is tolerated; they amount to concerted practices between authorities which act in the exercise of their discretion and which are therefore acts that are clearly not governed by international law’²⁷.

However, empowering freedom, security, and justice agencies to communicate personal data to third parties through administrative instruments, as the DPREU foresees, must not go beyond each agency’s operational mandate while respecting the limits established by the post-*Meroni* jurisprudence.

3.2. Methodology

The methodology applied in this work follows the disciplinary approach of legal dogma, or juridical science. Different hermeneutic techniques are used: The abductive method helps us inspect the actual reach of the IO Regulations both internally and externally; analytical, or deductive, reasoning turns out to be indispensable to assess the consistency of Article 50 of the IO Regulations with the general framework of the GDPR, the LED, and the EUDPR; the inductive method is useful to infer that the IO Regulations pursue a new identity or case management model, for example.

The dissertation is based on primary resources gathered between 2019 and 2022. Some primary resources are elaborated on through a quantity approach and include: first, structured and semi-structured interviews conducted between 2020 and 2022; and, second, the Ph.D. candidate’s empirical knowledge acquired during her research period at the European Commission. Several surveys were carried out in Brussels, these mainly took place online because of COVID-19, and included interviews with:

²⁶ Renaud Dehousse, “Delegation of Powers in the European Union: The Need for a Multi-Principals Model”, *West European Politics*, Vol. 31, No. 4, 2008, pp. 789-805.

²⁷ Opinion of Advocate General Tesauro, C-327/91, *French Republic v Commission of the European Communities*, 16 December 1993, EU:C:1993:941, para. 22. See also C-66/13, *Green Network Spa v Autorità per l’energia elettrica e il gas*, 26 November 2014, EU:C:2014:2399, extending the *AETR/ERTA* effect to agreements concluded by Member States and third countries’ administrative authorities, and Florin Coman-Kund, “EU agencies as global actors: a legal assessment of Europol’s international dimension”, *Maastricht Faculty of Law Working Paper*, No. 6, 2014, pp. 1-43.

- seven officials from Director General of Migration and Home Affairs (DG HOME) working on the implementation of the interoperability reforms, on large-scale IT systems, on forgery or theft of documents, and on return of third-country nationals;
- one official from the European Return and Reintegration Network (ERRIN);
- one official from the EBCG Agency;
- one official from Europol, and
- one official from eu-LISA.

In addition, a questionnaire on interoperability was submitted to the DG HOME's leading research expert. Empirical material was elaborated when the Ph.D. candidate worked at the European Commission, in the DG HOME-B3 Unit, from February 2020 until February 2021. During this period, the Ph.D. candidate performed the following tasks:

- legal support on the interpretation of Regulations (EU) 2019/817 and 2019/818 and the co-related large-scale IT systems;
- legal drafting of the secondary legislation following Regulations (EU) 2019/817 and 2019/818;
- reporting on meetings with different stakeholders (Council of the EU, Member States, Union agencies, Interoperability Committee, Interoperability Expert Group, eu-LISA Advisory Group, and so on);
- preparing training materials, including documents and presentations, and
- leading the drafting of the Interoperability Handbook.

Other primary sources of material include: literature (books, dissertations, peer-reviewed scientific journals, journals, reports, and papers); international, supranational, and national law (principles and positive rules) as well as jurisprudence, and official soft law documents. The information has been retrieved through the use of specific keywords according to the following macro-fields: human rights; privacy and data protection; EU external relations; AFSJ; Union agencies; large-scale IT systems, and interoperability. These resources are approached through a qualitative lens, which grants a holistic view on the juridical problems posed by the research object.

Secondary sources of material were the legal databases of the University of Granada (Spain), the University of Ferrara (Italy), the European Commission Library (Belgium), and the Peace Palace Library (The Netherlands). Open-source platforms – e.g., Dialnet and Google Scholar – and public webpages – e.g., ec.europa.eu, consilium.europa.eu, europarl.europa.eu – have also been consulted.

3.3. Content

The dissertation develops across six chapters. The first two Chapters focus on the EU normative competence on the protection of personal data and on the free movement of such data embedded in Article 16 of the TFEU and the corresponding fundamental right to the protection of personal data consecrated in Article 8 of the CFREU. The analysis is based on the EU's competence system underpinned by the principle of conferral under the assumption that this principle represents the keystone around which any international organisation regulates its internal and external action. This is particularly relevant to the EU, where the protection of fundamental rights is relegated to the implementation of Union policies. In this preliminary phase, we will assess the principles underpinning the EU data protection *acquis* and whether these apply to the AFSJ. Indeed, the adoption of the LED for PJCCM suggests that such an *acquis* suffers from a sectoral approach that introduces important derogations for the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties. If this is the case, different regimes on the transfer of personal data might coexist depending on the purpose of its transfer. The communication of personal data to foreign partners is regulated by a complex legal framework made of rules and principles that modulate the EU's external activity based on Article 16 of the TFEU, even when this legal basis is implicit within the realm of cooperation on freedom, security, and justice issues. Consequently, our analysis will not be limited to the dispositions regulating the transfer of personal data within the EU's legislation, which already establishes a set of principles to be respected regarding the processing of personal data, but it also extends to the legal framework applicable to the EU's external activity, that is, the international and supranational rules that guide its intervention as a global player. Specifically, we will consider the theory on the implied external competences of international organisations to clarify whether, and if so how, the EU is empowered to regulate the communication of personal data beyond the Union's borders. Both in the normative and in the operational layer, the transfer of personal data to third parties must respect human and fundamental rights consecrated in international instruments that bind the EU and its Member States.

The third and fourth Chapters analyse the evolution of the six large-scale IT systems that integrate with the interoperability infrastructure until their institutionalisation according to the delegation doctrine as reformulated by the CJEU. Large-scale IT systems have been implemented according to specific freedom, security, and justice policies, but they risk being

confused with each other due to the nature of the interoperability project. Such implementation responds to the principle of conferral that requires the Union to respect the horizontal boundaries foreseen in the founding Treaties. However, centrally stored personal data could easily be accessed by different authorities and Union staff pursuing other objectives and responding to a different conferred competence. Uncontrolled access to the personal data stored in large-scale IT systems might be found to be incompatible with the principles regulating the processing of personal data, among which the principle of purpose limitation stands out. It is not clear how competence and data protection approaches interrelate with one another and if their complex relationship paved the way for the adoption of the IO Regulations. Let us assume that the principle of purpose limitation has been weakening the policy-to-policy boundaries traced by the founding Treaties, which eu-LISA's mandate shows. Union agencies enable the implementation of shared competences thanks to the cooperation of EU officials and Member States' national authorities while avoiding the centralisation of executive powers in the European Commission's hands. Thus, the institutionalisation of the EU's operational competence in the management of large-scale IT systems could have represented a crucial step in unblocking the interoperability reform that was first proposed after 11-S. If eu-LISA is assigned tasks to develop, implement, and monitor the interoperability infrastructure, the revised *Meroni* jurisprudence has defined the limits to the delegation of such competences to other bodies. Currently, it is not clear whether this new agency has been granted access to personal data and, consequently, if it could be responsible for transferring such data to third countries and international organisations.

The fifth and sixth Chapters inspect the circumstances around the creation of the IO Regulations, their content, purposes, and external scope. Before analysing their external dimension, the circumstances, content and purposes of the sister Regulations is explored to highlight whether the IO Regulations bring any added value to the underlying large-scale IT systems. Regulations (EU) 2019/817 and 2019/818 establish four new components that could serve to achieve the interoperability objectives. These components are: the European Search Portal (ESP); the shared Biometric Matching Service (sBMS); the Common Identity Repository (CIR), and the Multiple-Identity Detector (MID). In addition, the Regulations foresee that a Common Repository for Reports and Statistics (CRRS) should be established. Thus, we assume that interoperability is equipped with its own set of goals that enrich those pursued by the systems themselves. Such an inspection is indispensable in order to understand how the new IT architecture could facilitate the interconnection of foreign databases, which we will analyse in the last Chapter. Article 50 will be addressed while

taking into account: first, that different degrees of interoperability can be established depending on the legal basis with which personal data is being transferred; and, second, that national authorities, Union agencies and large-scale IT systems might transfer personal data with or without human intervention. Our analysis will shed light on the terms in which interoperability with foreign databases is lawful and sustainable – i.e., consistent – according to the principles and rules analysed in the previous Chapters. However, we will not address the communication of personal data to private parties through the interoperability components – e.g., to air carriers – since this aspect has not been fully regulated by the co-legislators yet.

4. The “who”, “when” and “where” of the research

The dissertation was undertaken by Francesca Tassinari from 2019 to 2022 period: The first and the second years were used to collect bibliographic sources. Between 2020 and 2021, the Ph.D. candidate lived and studied in Brussels and Ferrara; the writing phase was completed in spring 2022. The research has been funded by the Spanish Ministry of Education, Culture and Sport, and the Vice-rectorate for Research and Transference of the University of Granada. The European Commission covered part of the costs of the research period in Brussels.

INTRODUCCIÓN

1. El “qué” de la investigación

1.1. Antecedentes

En mayo de 2019, la Unión Europea (UE) adoptó un marco sobre la interoperabilidad entre los sistemas de tecnología informática (TI) en materia de fronteras, visados, cooperación policial y judicial penal, asilo y migración. Los Reglamentos (UE) 2019/817¹ y 2019/818² (Reglamentos IO) se proponen interconectar los seis sistemas TI ya existentes o de pronta implementación en el Espacio de Libertad, Seguridad, y Justicia (ELSJ) bajo el auspicio de una nueva arquitectura que soportará su funcionamiento. Estos sistemas son: el Sistema de Información Schengen (SIS); el Sistema de Información de Visados (VIS); el Sistema de Entrada y Salida (SES); el Sistema de Información y Autorización de Viajes (SEIAV); el sistema de Dactiloscopia Europea (Eurodac), y el Sistema centralizado para la identificación de los Estados miembros que poseen información sobre condenas de nacionales de terceros países y apátridas (ECRIS-TCN). La interoperabilidad se define como la habilidad de los sistemas de comunicar la información previamente almacenada en “bases de datos” centralizadas y compartidas. Sin embargo, el lenguaje altamente técnico usado por el legislador ha sido duramente criticado por quienes ponen en duda el hecho de que esta definición refleje su verdadero alcance que, a día de hoy, sigue siendo una incógnita.

Cuando la interoperabilidad se extiende por distintos ordenamientos jurídicos permite que la información y los datos personales³ fluyan entre distintas jurisdicciones. Según el Prof. Palfrey y el Prof. Gasser:

¹ Reglamento (UE) 2019/817 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los visados y por el que se modifican los Reglamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 y (UE) 2018/1861 del Parlamento Europeo y del Consejo, y las Decisiones 2004/512/CE y 2008/633/JAI del Consejo, PE/30/2019/REV/1, *DO L* 135 de 22.5.2019, pp. 27-84.

² Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración y por el que se modifican los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816, PE/31/2019/REV/1, *DO L* 135 de 22.5.2019, pp. 85-135.

³ Esta tesis no pretende trazar una línea de demarcación entre “datos personales” e “información” porque en el marco de la interoperabilidad los datos relacionados con la persona – incluidos los que sirven para identificarla inequívocamente – juegan un papel fundamental respecto al resto de la información.

«One of the primary benefits of interoperability is that it can preserve key elements of diversity while ensuring that systems work together in the ways that matter most»⁴.

En 2012⁵, Bruening avanzó la idea de que la «interoperabilidad» podría asegurar el flujo de información también cuando existieran distintos enfoques culturales respecto al derecho de privacidad⁶. Según la autora, cualquier solución a los conflictos entre distintos escenarios culturales debería respetar la existencia de distintos conceptos de privacidad, en regímenes nacionales y regionales. En este sentido, la «interoperabilidad jurídica» se presenta como una alternativa a la armonización normativa, permitiendo la «compatibilidad» de distintos sistemas jurídicos, sin necesidad de acercar las legislaciones domésticas. En concreto, Bruening afirma que la interoperabilidad debería apoyarse sobre tres elementos:

1. principios comunes;
2. rendición de cuentas, y
3. cooperación entre las partes reguladoras.

De forma paralela, la Casa Blanca⁷ especificó que una interoperabilidad “global” no debería basarse en la protección común de los derechos humanos, sino en el reconocimiento mutuo y en la ejecución del principio de cooperación: el primero se fundamenta en la presunción de que otros sistemas jurídicos con «valores comunes en materia de privacidad y de protección de datos personales»⁸; el segundo requiere que el sujeto responsable de la actividad de tratamiento de datos rinda cuenta por su actividad.

⁴ John Palfrey y Urs Gasser, *Interop. The Promise and Perils of Highly Interconnected Systems*, EE.UU., Basic Books, 2012, p. 11.

⁵ Paula J. Bruening, “Interoperability: analysing the current trends & developments”, *Data protection law & policy*, 2012, pp. 12-14.

⁶ De forma similar, Amedeo Santusuoosso y Alessandra Malerba, “Legal Interoperability as a Comprehensive Concept in Transnational Law”, *Law, Innovation and Technology*, Vol. 6 No. 51, 2014, pp. 51-73, p. 68, afirman: «[...] legal interoperability is able to explain some legal phenomena that are very different in kind and to encompass them in a unique conceptual frame». Esto conlleva que de forma diferente que las disciplinas comparatistas que quieren uniformar, la interoperabilidad jurídica está dirigida a: focalizarse en las diferencias más que sobre las similitudes; poner en contacto (y hacer operativos) elementos que naturalmente estarían separados por algunos despistes conceptuales o lingüísticos, y ofrecer una visión de más de dos partículas/sistemas legales que trabajan conjuntamente.

⁷ The White House, *Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy*, Washington D.C., 2012, p. 31 y ss.

⁸ Torben Holvad, “Mutual recognition, standards and interoperability”, en Matthias Finger y Pierre Messulam, *Rail economics, regulation and policy in Europe*, Cheltenham, Edward Elgar Publishing, 2015, pp. 275-302, p. 280:

«The principle of mutual recognition is fundamental to the functioning of the EU Single Market and the free movement of goods within the European Union. It establishes that: Member States must allow a product that has been lawfully produced and marketed in another Member State into their own market. This is the case even if the product does not comply with the technical rules in that country. The mutual recognition principle can only be disregarded by a Member State in case of overriding general interest, such as that relating to public health or environmental protection [...]».

A pesar de esto, en el contexto de la UE, la transferencia de datos personales que no está respaldada por estándares de armonización normativos puede infringir las garantías establecidas en la legislación de la Unión en materia de protección de datos personales, ya que esta, de forma general, requiere que el estado tercero o la organización internacional aplique un nivel de protección “equivalente” al de la UE. El derecho humano a la *privacy*, en sus conceptualizaciones multifacéticas, y el derecho fundamental a la protección de los datos personales consagrado por primera vez en la Carta de Derechos Fundamentales de la Unión Europea⁹ (CDFUE), podrían verse menoscabados cuando la puesta a disposición de la información de un individuo constituye una injerencia desproporcionada. Después del escándalo Snowden¹⁰, incluso sistemas que se consideraban “ceranos” al modelo europeo, se examinan con desconfianza porque han sido juzgados como incompatibles con la escala de valores de la Unión. Por consiguiente, una “interoperabilidad global” debería sopesarse a la luz de los derechos de los individuos de forma cuidadosa.

Según el art. 50 de los Reglamentos hermanos, la comunicación de datos personales a países terceros, organizaciones internacionales y partes privadas se regula por los regímenes sobre transferencia de datos personales subyacentes de los sistemas TI de gran escala y de las agencias de la Unión. Además, los Reglamentos IO avanzan la conclusión de un Acuerdo de Cooperación con la Organización Internacional de Policía Criminal (Interpol) que conectaría la interoperabilidad con las bases de datos de Interpol sobre Documentos de Viaje Robados y Perdidos (SLTD) y Documentos de Viaje Asociados a Notificaciones (TDAWN). El art. 50 establece:

«Sin perjuicio del artículo 31 del Reglamento (CE) n.º 767/2008, los artículos 25 y 26 del Reglamento (UE) 2016/794, el artículo 41 del Reglamento (UE) 2017/2226 y el artículo 65 del Reglamento (UE) 2018/1240 y de la consulta de bases de datos de Interpol a través del PEB de conformidad con el artículo 9, apartado 5, del presente Reglamento que sean conformes a el capítulo V del Reglamento (UE) 2018/1725 y el capítulo V del Reglamento (UE) 2016/679, los datos personales almacenados en los componentes de interoperabilidad o tratados por ellos o a los que se acceda a través de esos componentes no se transmitirán ni se pondrán a disposición de terceros países, organizaciones internacionales ni entidades privadas».

Los colegisladores han presentado la interoperabilidad como una solución eficiente y efectiva para alcanzar objetivos de libertad, seguridad y justicia. De hecho, las reglas a las que se refiere el artículo sobre comunicación de datos se remite al *acquis* de la UE sobre protección de datos, o sea: el Capítulo V del Reglamento sobre protección de datos para las

⁹ Carta de los Derechos Fundamentales de la Unión Europea, DO C 326 de 26.10.2012, pp. 391-407.

¹⁰ Edward Snowden traducido por Esther Cruz Santaella, *Vigilancia Permanente*, Barcelona, Planeta, 2019.

instituciones, órganos, organismos de la UE¹¹ (EUDPR); el Capítulo V del Reglamento general de protección de datos¹² (RGPD), y (eventualmente) el Capítulo V de la Directiva sobre protección de datos para las autoridades de policía¹³ (LED). No obstante, no está claro si y en qué términos la dimensión externa de la interoperabilidad consigue respetar los parámetros normativos establecidos en el Derecho internacional y en el Derecho de la UE: ¿Se respetan, se eluden, o se incumplen con la interoperabilidad las normas y principios aplicados por la UE a la comunicación de datos personales a terceros en sus relaciones exteriores?

1.2. Objetivo y preguntas de investigación

1.2.1. Objetivo principal y pregunta de investigación subyacente

El objetivo principal de la investigación propuesta es determinar el alcance externo del marco de interoperabilidad establecido por los Reglamentos (UE) 2019/817 y 2019/818, eso es, su extensión más allá de las fronteras exteriores de la UE. Por consiguiente, el trabajo quiere analizar si la interoperabilidad de los sistemas centralizados de la UE con bases de datos extranjeras es legal y “sostenible” – i.e., coherente¹⁴ – respecto a las normas y principios que regulan la acción exterior de la UE. En concreto, valoraremos si el art. 50 de los Reglamentos IO cumplen con los marcos internacionales y supranacionales y, en su caso, si los derechos individuales, especialmente el derecho fundamental a la protección de los datos personales, están realmente garantizados.

¹¹ Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (Texto pertinente a efectos del EEE.), PE/31/2018/REV/1, DO L 295 de 21.11.2018, pp. 39-98.

¹² Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE), DO L 119 de 4.5.2016, pp. 1-88.

¹³ Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, DO L 119 de 4.5.2016, pp. 89-131.

¹⁴ Art. 7 de la Versión consolidada del Tratado de Funcionamiento de la Unión Europea, DO C 326 de 26.10.2012, pp. 47-390: «La Unión velará por la coherencia entre sus diferentes políticas y acciones, teniendo en cuenta el conjunto de sus objetivos y observando el principio de atribución de competencias».

1.2.2. Preguntas accesorias

Para contestar a la pregunta objeto de la investigación principal, debe responderse a las siguientes cuestiones accesorias:

1. ¿En qué consiste el *acquis* de la UE sobre protección de datos y cómo se regula en el ELSJ?
2. ¿Cómo se regula la protección y la transferencia de datos personales en la UE?
3. ¿Cómo y con qué finalidades tratan datos personales los sistemas TI de gran magnitud?
4. ¿Qué rol tiene la Agencia de la Unión Europea para la gestión operativa de sistemas TI de gran magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA)?
5. Además de perseguir la interconexión de los sistemas TI de gran magnitud, ¿cuáles el verdadero alcance – i.e., circunstancias, objetivos, contenidos – del marco de interoperabilidad?
6. ¿Cómo se relaciona la interoperabilidad de los sistemas TI de gran magnitud con la competencia exterior de la UE en materia de protección de datos personales y la libre circulación de estos datos?

1.3. Hipótesis

Para contestar a la pregunta principal sobre el objeto de la investigación, suponemos que el alcance externo de la interoperabilidad tiene diferentes matices. En primer lugar, cabe destacar que la dimensión externa de la interoperabilidad no debería reducirse a una función de soporte de los sistemas TI de gran magnitud subyacentes y de las agencias, sino que – además de la interconexión de las bases de datos de Interpol que está expresamente prevista – el art. 50 de los Reglamentos IO prevé nuevas formas y canales de comunicación de los datos personales hacia terceras partes. De lo contrario, esta norma no aportaría ningún valor añadido a las normas sobre transferencia de datos previstas por los sistemas TI de gran magnitud subyacentes. En concreto, avanzamos la hipótesis de que el art. 50 de los Reglamentos IO permitiría la interoperabilidad de las bases de datos de países terceros y organizaciones internacionales con los componentes de la Unión para mejorar la capacidad operativa de la Unión en el ELSJ, tanto en su dimensión interna como en la externa. Esta hipótesis requiere analizar el ámbito de aplicación interno de la interoperabilidad, así como

su valor añadido respecto a los objetivos perseguidos por los sistemas TI de gran magnitud relevantes.

Sobre esta base, proponemos una segunda hipótesis de investigación según la cual, distintos grados de interoperabilidad pueden ser regulados en términos de interconexión directa y de legibilidad de los datos. Esta tesis se funda en un concepto amplio de la definición de “transferencia de datos” que incluye múltiples mecanismos para poner los datos a disposición de terceros – e.g., el «intercambio de datos personales» o la «puesta a disposición de datos personales» –, y que contempla las peculiaridades que derivan del régimen de protección de datos aplicable en el ELSJ. En definitiva, nuestro análisis no se refiere a una interpretación literal sino sistemática del art. 50. Tomando en consideración la evolución técnico-política de los sistemas TI de gran magnitud de los pasados veinte años, deberíamos apreciar que las agencias del ELSJ con acceso a la arquitectura de interoperabilidad – Agencia de la Unión Europea para la Cooperación Policial (Europol), Agencia de la Unión Europea para la Cooperación en materia de Justicia Penal (Eurojust), Agencia Europea de Guardia Fronteras y Costas (Agencia EGFC) y Agencia de Asilo de la Unión Europea (AAUE) – acceden a los datos almacenados de forma centralizada y pueden compartirlos por acuerdos administrativos de derecho duro o blando celebrados entre sí, así como con terceros países y organizaciones internacionales.

Nuestra premisa sugiere que la legalidad y sostenibilidad de cualquier tipo de interoperabilidad debe deducirse mediante un estudio realizado caso por caso en virtud de los principios y normas que regulan la acción exterior de la UE en materia de protección de datos. La comunicación de datos personales, realizada ya sea mediante máquinas que por seres humanos, debe respetar el marco legal que regula la acción exterior de la UE – o sus órganos –, incluida la CDFUE a la que está sujeta. Estas garantías no deben ser eludidas en vista de un mayor grado de orden y seguridad dentro del ELSJ. Visto que se espera que el marco de interoperabilidad afecte más a los migrantes de terceros países que a los ciudadanos de la UE, se necesitarían garantías apropiadas para hacer frente a las situaciones de vulnerabilidad y, en concreto, para prevenir cualquier forma de tratamiento discriminatorio, restricción o represión ilegal. Creemos que, en la práctica, la protección de algunos grupos de personas – e.g., menores y solicitantes de asilo – se vería afectada.

A esta altura, nuestra investigación debe completarse para contemplar la posibilidad de que el marco jurídico de la UE que regula la protección de los datos personales y su libre circulación pueda ser mejorado para acabar con situaciones de desprotección y lagunas legislativas. Analizar si el art. 50 de la interoperabilidad cumple con el *acquis* de la UE

podría no ser suficiente y se deberían avanzar propuestas *de lege ferenda* para que sea posible alcanzar los objetivos de libertad, seguridad y justicia con la protección transfronterizas de los derechos fundamentales.

2. El “porqué” de la investigación

Desde finales de los años 90, la evolución experimentada en el sector TI ha ido transformando la comunidad internacional en un mundo globalizado e interconectado. La difusión y la mejora de la tecnología de computación y de la Inteligencia Artificial (IA), que lideran esta revolución sobre la base de la avalancha de información que difundimos cada día¹⁵, están poniendo de relieve preocupaciones de cara a la protección de los derechos humanos de todas las personas. Como señala el Supervisor Europeo de Protección de Datos (SEPD), las tecnologías de la información y la comunicación (TIC) plantean nuevos retos en la esfera privada de las personas, ya que los datos personales se procesan de distintas formas – recopilación, clasificación, filtración, transferencia o conservación de otro tipo –, lo que multiplica los riesgos de injerencias¹⁶.

Los Reglamentos IO han sido objeto de las reformas más recientes emprendidas por la Unión para salvaguardar la eficiencia en el área de la libre circulación, después de haber sufrido numerosas crisis. La urgencia de la reforma se debe a las amenazas continuas contra el Espacio Schengen, que ha llevado a la introducción de la interoperabilidad incluso antes de que la Comisaria Von Der Leyen anunciase la Estrategia Digital de la UE el pasado 9 de marzo de 2021¹⁷. Nos preguntaremos, entonces, si esta reforma tan intrusiva ha sido

¹⁵ Joint Research Centre Technical Report, *AI Watch: Beyond pilots: sustainable implementation of AI in public services*, Luxemburgo, 2021, p. 32 y ss.: «One of the most fundamental requirements of AI is data. By definition, AI relies on access being ensured to the “right” kind of data on which to perform its analyses, and which in most cases is augmented by the results of the analyses themselves. For many Public Sector organizations though, fulfilling this requirement is a challenge, due to **a variety of obstacles in obtaining data of the quality and format they require**». El Dictamen Preliminar del SEPD, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, Bruselas, 10.03.2014, p. 9, informa de que cada día se recogen 2,3 billones de gigabytes de datos que se combinan para generar servicios y cartografía global.

¹⁶ Véase: el Dictamen del SEPD sobre *Promoting Trust in the Information Society by Fostering Data Protection and Privacy*, Bruselas, 18.03.2010; el Resumen del dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión sobre «La Agenda Digital para Europa — Motor del crecimiento europeo», DO C 358 de 7.12.2013, pp. 17-18, y la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre protección de infraestructuras críticas de información - «Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia» {SEC(2009) 399} {SEC(2009) 400}, COM(2009) 149 final, Bruselas, 30.3.2009.

¹⁷ La estrategia está disponible en la página oficial de la Comisión Europea en el siguiente enlace www.ec.europa.eu. Nótese que «a Europe fit for the digital age» es uno de los objetivos políticos claves acordados en la Joint Declaration of the European Parliament, the Council of the European Union and the European Commission, *EU Legislative Priorities for 2022*, Bruselas, 2022.

adoptada con la suficiente cautela y sensibilidad, o si el legislador se ha aprovechado, por así decirlo, de la crisis humanitaria para promover un marco jurídico restrictivo de los derechos fundamentales de todas las personas – sobre todo migrantes.

La solución de “problemas antiguos” con mecanismos novedosos promueve los nuevos proyectos de investigación que habrán de analizar si el entorno digital está provisto de garantías adecuadas para proteger los derechos personales. Después del 11-S, los programas estadounidenses de *collect it all* – “coleccionalo todo” – demostraron que la vigilancia cibernética puede restringir el derecho a la *privacy* y, en el marco supranacional, el derecho a la protección de datos personales de los individuos de forma desproporcionada bajo el pretexto de combatir la criminalidad y el terrorismo. A partir de entonces, se percibe un clima de desconfianza hacia los servicios de inteligencia en todo el globo. El hecho de que el nuevo marco de interoperabilidad establecido por los Reglamentos (UE) 2019/817 y 2019/818 permita el flujo de datos hacia y desde terceras partes, incluidos sistemas jurídicos que protegen de forma diferente los derechos humanos, cuestionan la validez y la oportunidad de una “interoperabilidad global” ilimitada. Además, otros principios no derogables – e.g., la prohibición de discriminación y la de *refoulement* – se vuelven relevantes mientras que los grupos de migrantes vulnerables se ven afectados.

2.1. Estudios previos

Puesto que un primer intento de establecer un marco para la interoperabilidad dentro del ELSJ se remonta a las secuelas del 11-S, varios estudios relacionados con nuestro tema de investigación se han desarrollado a partir de los años 2000. En concreto, se reconocen dos olas de estudios académicos:

- un primer grupo de estudios se centra en la interoperabilidad entre los sistemas SIS, VIS, y Eurodac, aunque este proyecto fue descartado por razones legales, políticas, y técnicas;
- un segundo grupo de estudios se desarrolló después de la Comunicación de la Comisión Europea al Parlamento Europeo y al Consejo sobre Sistemas de Información más sólidos e inteligentes para la gestión de las fronteras y la seguridad de 6 de abril de 2016¹⁸ y que concierne a los Reglamentos IO y, más en general, a los sistemas TI de gran magnitud.

¹⁸ Comunicación de la Comisión al Parlamento Europeo y al Consejo, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final, Bruselas, 6.4.2016.

En ambos casos, la escuela belga dirigida por el Prof. De Hert ha sido pionera en el avance de los estudios de interoperabilidad dentro del ELSJ, y a ella se unieron después, por ejemplo, la escuela francesa del Prof. Bigo, la escuela holandesa de la Profa. Brouwer y, más recientemente, la londinense de la Profa. Vavoula. De esta última se espera la publicación de una importante monografía sobre sistemas TI de gran magnitud, poco después de la presentación de esta tesis.

2.2. Situación actual

Todas las contribuciones sobre el marco de interoperabilidad establecido por los Reglamentos (UE) 2019/817 y 2019/818 adoptan un único enfoque normativo interno: el de los derechos humanos. Primero, la interoperabilidad y los sistemas TI de gran magnitud se analizan frente a la protección del derecho humano a la privacidad y, aún más importante, del derecho fundamental a la protección de los datos personales consagrado en la CDFUE. Otros estudios, en cambio, evalúan el impacto de los Reglamentos hermanos sobre el individuo teniendo en consideración el hecho de que los datos personales que se vean afectados pueden ser tratados por parte de las agencias de la Unión y no solamente por las autoridades nacionales. Estas contribuciones aportan resultados parciales sobre el marco de la interoperabilidad y, en algunos casos, inducen a error a causa de la falta de una visión de conjunto de la reforma. En suma, la interoperabilidad ha sido analizada desde una sola perspectiva disciplinaria limitada y no contamos con una teoría plenamente desarrollada sobre la dimensión exterior de los Reglamentos (UE) 2019/817 y 2019/818. En definitiva, todos estos estudios tienen un valor inestimable porque han dejado constancia de las diferentes teorías que se aplican al marco de la interoperabilidad y que las teorías que abarcan su dimensión externa son aún más numerosas. El marco jurídico que se deriva de ello es complejo, pero hace que nuestra investigación sea lo más original posible.

3. El “cómo” de la investigación

3.1. Marco jurídico

Los cimientos de nuestra tesis se construyen sobre el liberalismo y el humanismo aplicado a una organización internacional concreta – i.e., la UE – que se basa en el respeto de los derechos humanos, la libertad individual, la diversidad, la solidaridad, y la democracia¹⁹.

¹⁹ Art. 2 de la versión consolidada del Tratado de la Unión Europea, *DO* C 326 de 26.10.2012, pp. 13-390 (TUE).

Como afirma el Prof. Liñán Nogueras, la UE goza de una personalidad jurídica limitada, condicionada por la voluntad de sus Estados miembros, y limitada en su finalidad y contenido, que son determinados por sus funciones²⁰. La configuración de un ordenamiento jurídico supranacional, que se mueve hacia la máxima integración posible de sus Estados miembros, permitió el desarrollo de un marco jurídico de «alto nivel de protección» de los datos personales, también para la Cooperación Penal y Judicial Penal (PJCCM), con resultados nunca alcanzados previamente. El liderazgo digital de la UE ha sido brindado en una nueva competencia atribuida a la UE desde 2007 para regular la protección de los datos personales y la libre circulación de estos datos, en el art. 16 del TFUE. Esta nueva competencia establece un puente con el derecho fundamental a la protección de los datos personales y el derecho a una vida privada de los arts. 8 y 7 de la CDFUE, que es vinculante desde el 2009.

No obstante, el hilo conductor de nuestra investigación debe encontrarse no solo en el *acquis* de la UE basado sobre el art. 16(2) TFUE, sino también en los principios y normas que la UE debe respetar en cuanto actor global sujeto al derecho internacional público cuando actúa externamente²¹. Por consiguiente, el alcance exterior de los Reglamentos IO debe analizarse bajo un enfoque competencial en virtud del régimen sobre la transferencia de datos personales del RGPD, de la LED, y del EUDPR. En concreto, debemos referirnos a la jurisprudencia *AETR/ERTA*²² del Tribunal de Justicia de la UE (TJUE), conforme al cual la Unión puede adquirir una competencia externa (implícita) para asegurar que los estándares internos no son eludidos cuando los datos personales se transfieran a autoridades extranjeras. La UE fue el primer actor en adoptar un modelo de “adecuación” o “basado en la geografía” que le otorga a la Comisión Europea el mandato de evaluar la compatibilidad de la legislación de terceras partes respecto a la de la UE. De conformidad con este régimen, la adopción de una decisión de adecuación debe preferirse a la conclusión de un tratado internacional y a las cláusulas de derogación. En el *Dictamen 1/15*²³, el TJUE aclaró que la transferencia de datos personales, conocida como Registro de Nombre de Pasajero (PNR),

²⁰ Véase Diego Javier Liñán Nogueras, “La acción de la Unión: las relaciones exteriores (I)”, en Araceli Mangas Martín y Diego Javier Liñán Nogueras, *Instituciones y Derecho de la Unión Europea*, Madrid, Tecnos, 2020, recurso en línea.

²¹ Por el contrario, nuestra investigación no se ocupa de los marcos internacionales y supranacionales de ciberseguridad, ya que el Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la cooperación reforzada y la divulgación de pruebas electrónicas, firmado en Estrasburgo el 12 de mayo de 2022, y la estrategia de la UE en materia de ciberdelincuencia estaban en revisión.

²² C/22-70, *Comisión de las Comunidades Europeas contra Consejo de las Comunidades Europeas. Acuerdo europeo sobre transportes por carretera*, 31 de marzo de 1971, EU:C:1971:32.

²³ *Dictamen 1/15*, 26 de julio de 2017, EU:C:2017:592.

hacia un país tercero debe ser regulada en un acuerdo internacional bajo los arts. 87(2)(a) y 26(2) del TFUE, para cubrir las medidas en materia de transferencia y protección de datos respectivamente. Si consideramos que el conjunto de normas sobre la protección de los datos personales que regula su transferencia es el resultado del ejercicio de la competencia de la UE sobre protección de datos personales y sobre su libre circulación basada en el art. 16(2) TFUE, es necesario examinar igualmente su dimensión externa, analizando la relación entre las decisiones de adecuación y los acuerdos internacionales.

En realidad, este marco jurídico se aplica ya sea cuando la Unión actúa directamente como cuando la Unión delega la ejecución de sus competencias en otros organismos y agencias. Visto que el segundo pilar sobre el cual construiremos la dimensión externa de la interoperabilidad estará integrado por las agencias de la Unión que tienen acceso a la nueva infraestructura TI, una segunda teoría fundamental que guiará nuestra investigación es la doctrina de la delegación de poderes. En concreto, la jurisprudencia *Meroni*²⁴ complementa la teoría de los poderes implícitos, en la medida en que a las agencias de la Unión se les delega la conclusión de acuerdos administrativos de derecho duro y blando ante la necesidad de alcanzar objetivos internos por medio de la cooperación con autoridades extranjeras. La teoría de las relaciones exteriores de la UE se basa en el principio fundamental de atribución de competencias que obliga a la UE, y a sus instituciones, a actuar dentro de los límites establecidos por los Tratados fundacionales – o sea, en razón de las bases jurídicas expresas que se contemplan en los Tratados que confieren a la UE el poder de actuar externamente o, en su ausencia, por medio de la teoría de las competencias implícitas²⁵. La doctrina *Meroni* revisitada impone a la autoridad “principal”²⁶ de “traspasar su responsabilidad” al órgano delegado para que efectivamente se dé la delegación de poderes. La acción exterior de las agencias de la Unión se limita a los denominados acuerdos técnico-administrativos de derecho duro o blando, siendo estos implementación de los tratados concluidos sobre la base del art. 218 TFUE o, en general, como implementación de la legislación de la UE. Como recordó el Abogado General Tesauro:

«[...] el Derecho internacional conoce los acuerdos vinculantes y, todo lo más, la peculiar categoría de los acuerdos no vinculantes, calificados de manera variada y pintoresca, pero que pueden resumirse en dos supuestos básicos: los “gentlemen's

²⁴ C/9-56, *Meroni & Co., Industrie Metallurgiche, SpA contra Alta Autoridad de la Comunidad Europea del Carbón y del Acero*, 13 junio 1958, EU:C:1958:7.

²⁵ Jacopo Alberti, *Le Agenzie dell'Unione Europea*, Milano, Giuffrè, 2018, p. 33 y ss., p. 419: «[...] le agenzie i cui regolamenti istitutivi non prevedono la competenza ad agire a livello internazionale non sono sempre esentate dal farlo [...]».

²⁶ Renaud Dehousse, “Delegation of Powers in the European Union: The Need for a Multi-Principals Model”, *West European Politics*, Vol. 31, No. 4, 2008, pp. 789-805.

agreements”, que en ocasiones pueden cobrar un gran valor político e incluso estar dotados de un mecanismo de control internacional para su observancia, y los “pactos” destinados a consolidar orientaciones o líneas de conducta en determinados sectores, pero que carecen de todo valor jurídico, como a menudo manifiesta la explícita voluntad de las partes. No creo superfluo subrayar aquí que dichos acuerdos son normalmente concluidos por las autoridades competentes para ello y por ninguna otra autoridad ni Institución»²⁷.

Sin embargo, delegar en las agencias del ELSJ la competencia para comunicar datos personales a terceras partes mediante instrumentos administrativos, como hace el EUDPR, no debe desbordar el mandato conferido a cada agencia y no debe sobrepasar los límites establecidos por la jurisprudencia post-*Meroni*.

3.2. Metodología

La metodología aplicada sigue el enfoque disciplinario de la dogmática jurídica, o ciencia jurídica. Se utilizan diferentes técnicas hermenéuticas: el método abductivo nos ayuda a inspeccionar el alcance real de los Reglamentos IO tanto a nivel interno como externo; el razonamiento analítico o deductivo resulta indispensable para evaluar la coherencia del art. 50 del Reglamento IO con el marco general del RGPD, de la LED y del EUDPR; el método inductivo, en cambio, es útil para inferir que los Reglamentos IO persiguen un nuevo modelo de identidad o de gestión de casos, por ejemplo.

La tesis se basa en recursos primarios recogidos en el periodo 2019-2022. Algunos recursos primarios se elaboran mediante un enfoque cuantitativo y contemplan: en primer lugar, entrevistas estructuradas y semiestructuradas realizadas entre 2020 y 2022; en segundo lugar, el conocimiento empírico de la doctoranda adquirido durante su periodo de investigación en la Comisión Europea. Se realizaron varias encuestas en Bruselas, principalmente en línea debido a la COVID-19, a:

- siete funcionarios de la Dirección General de Migración y Asuntos de Interior (DG HOME) que trabajan en la aplicación de la reforma de la interoperabilidad, en los sistemas TI de gran magnitud, en la falsificación o el robo de documentos y en el retorno de los nacionales de terceros países;
- un funcionario de la Red Europea de Retorno y Reintegración (ERRIN);
- un funcionario de la Agencia EGFC;
- un funcionario de Europol, y
- un funcionario de eu-LISA.

²⁷ Conclusiones del Abogado General Tesauro, C-327/91, *República Francesa contra Comisión de las Comunidades Europeas*, 16 de diciembre de 1993, EU:C:1993:941.

Asimismo, se presentó un cuestionario sobre interoperabilidad al máximo experto de la DG HOME en el ámbito de la investigación. El material empírico se elaboró durante el periodo de investigación en la Comisión Europea, en la Unidad DG HOME-B3, desde febrero de 2020 hasta febrero de 2021. Concretamente, la doctoranda realizó las siguientes tareas:

- apoyo jurídico en la interpretación de los Reglamentos (UE) 2019/817 y 2019/818 y de los sistemas TI de gran magnitud conexos;
- redacción jurídica del derecho derivado tras los Reglamentos (UE) 2019/817 y 2019/818;
- información de las reuniones con las diferentes partes interesadas (Consejo de la UE, Estados miembros, agencias de la Unión, Comité de Interoperabilidad, Grupo de Expertos en Interoperabilidad, Grupo Consultivo de eu-LISA, etc.)
- preparación de materiales de formación, como documentos y presentaciones, y
- dirección de la redacción del Manual sobre interoperabilidad.

Otras fuentes primarias de material utilizadas son: la literatura (libros, tesis, revistas científicas revisadas por pares, periódicos, informes y documentos); el derecho internacional, supranacional y nacional (principios y normas positivas), así como la jurisprudencia, y los documentos oficiales de derecho blando. La información se ha recuperado mediante el uso de palabras clave específicas según los siguientes macro-campos de estudio: derechos humanos; privacidad y protección de datos; relaciones exteriores de la UE; ELSJ; agencias de la Unión; sistemas TI de gran magnitud, e interoperabilidad. Estos recursos se abordan a través de un enfoque cualitativo que otorga una visión holística de los problemas jurídicos objetos de nuestra investigación.

Las fuentes secundarias son las bases de datos jurídicas de la Universidad de Granada (España), la Universidad de Ferrara (Italia), la Biblioteca de la Comisión Europea (Bélgica), y la Biblioteca del Palacio de la Paz (Holanda). También se han consultado plataformas de código abierto – por ejemplo, Dialnet y Google Académico – y páginas web públicas – por ejemplo, ec.europa.eu, consilium.europa.eu, europarl.europa.eu.

3.3. Contenido

La tesis se estructura en seis capítulos. Los primeros dos Capítulos se concentran en la competencia normativa de la UE sobre la protección de los datos personales y sobre la libre circulación de estos datos en virtud del art. 16 del TFUE y el derecho fundamental correspondiente a la protección de los datos personales consagrado en el art. 8 de la CDFUE.

El análisis se basa en el sistema de competencias de la UE que se sustenta en el principio de atribución de competencias bajo el auspicio de que este principio integre la piedra angular de cualquier organización internacional, en sus relaciones internas y externas. Esto es especialmente relevante para la UE donde la protección de derechos fundamentales es relegada a la implementación de las políticas de la Unión solamente. En una fase preliminar, valoraremos los principios que fundamentan el *acquis* de la Unión sobre protección de datos y si estos se aplican al ELSJ en su conjunto. De hecho, la adopción de la LED para PJCCM sugiere que el *acquis* sufre de una aplicación sectorial que introduce derogaciones importantes para la prevención, investigación, detección, o prosecución de delitos criminales o la ejecución de penas. En su caso, distintos regímenes sobre la transferencia de datos personales coexistirían dependiendo de la finalidad del tratamiento. La comunicación de datos personales a partes extranjeras se regula bajo un marco jurídico complejo de principios y derechos que modulan la acción exterior de la UE basada en el art. 16 del TFUE, incluso cuando esta base jurídica es eclipsada por la cooperación basada en el ELSJ. Por consiguiente, nuestro análisis no se limitará a las disposiciones que regulan la transferencia de datos personales dentro del ordenamiento de la UE, que ya de por sí prevén una serie de principios a respetar para el tratamiento de datos personales, sino que se extenderá al marco jurídico aplicable a la UE en sus relaciones exteriores, eso es, las normas internacionales y supranacionales que guían su presencia como actor global. En concreto, consideraremos la teoría de los poderes implícitos de las organizaciones internacionales para aclarar si y cómo la UE cuenta con la competencia para regular la comunicación de datos personales más allá de las fronteras de la Unión, tanto en el plano normativo como en el operativo. La transferencia de datos personales a terceras partes debe respetar los derechos, humanos y fundamentales, previstos en los instrumentos que vinculan a la UE y a sus Estados miembros.

Los Capítulos tercero y cuarto analizan la evolución de los seis sistemas TI de gran magnitud porque estos integran la infraestructura de la interoperabilidad, así como su institucionalización de conformidad con la doctrina de delegación de poderes formulada por el TJUE. Los sistemas TI de gran magnitud han sido implementados de conformidad con políticas específicas del ELSJ, pero pueden terminar confundándose entre ellas en el marco de la interoperabilidad. Esa implementación se debe al principio de atribución que impone a la Unión respetar la subdivisión horizontal de competencias de acuerdo con los Tratados fundacionales. Sin embargo, las autoridades y el personal de la Unión pueden acceder a los datos personales almacenados centralmente en razón de sus distintas y variadas competencias. El acceso sin un control específico a los datos personales almacenados en los

sistemas TI de gran magnitud puede ser contrario a los principios de tratamiento de datos personales, entre los cuales se recuerda el principio de limitación de la finalidad del primer tratamiento. No está claro cómo los enfoques de la atribución de la competencia y de protección de datos interactúan entre ellos y cómo esta interacción ha abierto el paso a los Reglamentos IO. Supongamos que el principio de la primera finalidad del tratamiento ha distorsionado los límites trazados entre cada política de la Unión de conformidad con los Tratados fundacionales, tal y como testimonia el mandato de eu-LISA. Las agencias de la Unión permiten la implementación de competencias compartidas gracias a la cooperación de los funcionarios de la UE y de las autoridades nacionales de los Estados miembros. Por ello, la institucionalización de la competencia operativa de la UE en la gestión de sistemas informáticos TI de gran magnitud podría haber representado un paso crucial para desbloquear la reforma de la interoperabilidad que se propuso por primera vez tras el 11-S. En el caso de que se asignen a eu-LISA tareas de desarrollo, implementación y seguimiento de la infraestructura de interoperabilidad, la jurisprudencia *Meroni* revisada definirá los límites de la delegación de dicha competencia a otros organismos. A día de hoy, no se sabe si esta agencia tiene acceso a los datos personales y, por ende, puede ser responsable por transferir datos hacia terceros países y organizaciones internacionales.

Los Capítulos quinto y sexto analizan las circunstancias, el contenido, los objetivos y la dimensión externa de los Reglamentos IO. Antes de analizar esta última, la dimensión interna de los Reglamentos hermanos será examinada para evidenciar si los Reglamentos IO aportan un valor añadido a los sistemas TI de gran magnitud subyacentes. Los Reglamentos (UE) 2019/817 y 2019/818 establecen cuatro nuevos componentes que sirven para alcanzar los objetivos de la interoperabilidad. Estos componentes son: un Portal Europeo de Búsqueda (PEB), un Servicio de Correspondencia Biométrica compartido (SCB compartido), un Registro Común de Datos de Identidad (RCDI), y un Detector de Identidades Múltiples (DIM). Los Reglamentos prevén también la implementación de un Repositorio Central para la presentación de Informes y Estadísticas (RCIE). De ahí que avancemos la idea de que la interoperabilidad está dotada de un conjunto de objetivos propios, diferentes de los perseguidos por los propios sistemas. Esta inspección es indispensable para entender cómo la nueva infraestructura TI podría facilitar la interconexión con bases de datos extranjeras que se aborda en el último Capítulo. El art. 50 será analizado teniendo en cuenta que: primero, distintos grados de interoperabilidad pueden establecerse dependiendo de las bases jurídicas a las que los datos personales se transfieren; segundo, que tanto las autoridades nacionales, los sistemas TI de gran magnitud como las agencias de la Unión podrían

transferir datos personales dependiendo de si la intervención humana es necesaria o no. Nuestro análisis aclarará los términos en los que la interoperabilidad con bases de datos extranjeras es legal de acuerdo con los principios y reglas estudiados en los Capítulos anteriores. Sin embargo, no nos detendremos en analizar la comunicación de datos personales con partes privadas mediante los componentes de la interoperabilidad – por ejemplo, a los transportistas aéreos – ya que este aspecto aún no ha sido regulado en su totalidad por los legisladores.

4. Los “quién”, “cuándo”, y “dónde” de la investigación

La tesis ha sido elaborada por Francesca Tassinari en el período 2019-2022: el primer y el segundo año se destinaron a la recopilación de fuentes bibliográficas; entre 2020-2021, la doctoranda realizó estancias y estudios en Bruselas y en Ferrara; la fase final de redacción se completó en la primavera de 2022. Toda la investigación ha sido financiada por el Ministerio de Educación, Cultura y Deporte de España, y el Vicerrectorado de Investigación y Transferencia de la Universidad de Granada. La Comisión Europea cubrió parte de los gastos del periodo de investigación en Bruselas.

INTRODUZIONE

1. Il “cosa” della ricerca

1.1. Precedenti

Nel maggio del 2019, l'Unione europea (UE) ha adottato un quadro normativo sull'interoperabilità tra i sistemi d'informazione tecnologica (IT) in materia di frontiere, visti, cooperazione di polizia e cooperazione giudiziaria penale, asilo, e migrazioni. I Regolamenti (UE) 2019/817¹ e 2019/818² (Regolamenti IO) mirano a mettere in interconnessione sei sistemi su larga scala dell'UE, già esistenti o di pronta implementazione, nello Spazio di Libertà, Sicurezza, e Giustizia (SLSG) con il presupposto che una nuova architettura supporterà il loro funzionamento. Questi sistemi sono: il Sistema di Informazione Schengen (SIS); il Sistema di Informazione Visti (VIS); il Sistema di Ingressi/Uscite (EES); il Sistema di Informazione e Autorizzazione ai Viaggi (ETIAS); il sistema di Dattiloscopia Europea (Eurodac), e il sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di Paesi terzi e apolidi (ECRIS-TCN). L'interoperabilità si definisce come l'abilità dei sistemi di comunicare, scambiare i dati, e usare l'informazione previamente registrati in banche dati centralizzate e condivise. Tuttavia, il linguaggio altamente tecnico utilizzato dai co-legislatori ha sollevato dure critiche che mettono in discussione la sua vera portata che, ad oggi, è ancora confusa.

Estendendosi attraverso diversi ordinamenti giuridici, l'interoperabilità permette all'informazione e ai dati personali³ di fluire tra più giurisdizioni. Secondo il Prof. Palfrey e il Prof. Gasser:

¹ Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio, PE/30/2019/REV/1, *GU L* 135 del 22.5.2019, pp. 27-84.

² Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816, PE/31/2019/REV/1, *GU L* 135 del 22.5.2019, pp. 85-135.

³ Questa tesi non mira a tracciare una linea netta tra “dati personali” ed “informazioni” poiché, nel quadro dell'interoperabilità, i dati relativi alla persona – compresi quelli che servono a identificarla in modo inequivocabile – svolgono un ruolo preponderante rispetto al resto dell'informazione.

«One of the primary benefits of interoperability is that it can preserve key elements of diversity while ensuring that systems work together in the ways that matter most»⁴.

Nel 2012⁵, Bruening presentò l'idea per la quale l'«interoperabilità» potrebbe assicurare il flusso di informazioni anche laddove esistano diversi approcci culturali alla *privacy*⁶. Secondo l'autrice, qualsiasi soluzione tra contesti culturali divergenti dovrebbe rispettare l'esistenza di svariati concetti di riservatezza a livello nazionale e regionale. In questo senso, la «interoperabilità giuridica» è vista come un'alternativa all'armonizzazione normativa, che permette la «compatibilità» di diversi ordinamenti, senza che ci sia bisogno di armonizzare le legislazioni nazionali sottostanti. Nello specifico, Bruening afferma che l'interoperabilità deve basarsi su tre pilastri fondamentali:

1. principi comuni;
2. responsabilizzazione, e
3. cooperazione tra i legislatori.

In parallelo, la Casa Bianca⁷ ha specificato che un'interoperabilità “globale” dovrebbe basarsi, non sulla protezione comune dei diritti umani, ma sul principio del mutuo riconoscimento e quello dell'effettiva esecuzione del quadro cooperativo: il primo si fonda sulla presunzione che altri sistemi giuridici compiono con «valori comuni che accerchiano la riservatezza e la protezione dei dati personali»⁸; il secondo richiede al soggetto responsabile dell'attività di trattamento di dimostrare il proprio adempimento.

⁴ John Palfrey e Urs Gasser, *Interop: The Promise and Perils of Highly Interconnected Systems*, Stati Uniti, Basic Books, 2012, p. 11.

⁵ Paula J. Bruening, “Interoperability: analysing the current trends & developments”, *Data protection law & policy*, 2012, pp. 12-14.

⁶ In modo non diverso, Amedeo Santusuosso e Alessandra Malerba, “Legal Interoperability as a Comprehensive Concept in Transnational Law”, *Law, Innovation and Technology*, Vol. 6 No. 51, 2014, pp. 51-73, p. 68, affermano: «[...] legal interoperability is able to explain some legal phenomena that are very different in kind and to encompass them in a unique conceptual frame». Questo implica che, diversamente dalle discipline comparatistiche che mirano all'uniformazione, l'interoperabilità giuridica vuole: concentrarsi sulle differenze piuttosto che sulle somiglianze; mettere in contatto (e rendere operativi) elementi che naturalmente sarebbero separati a causa di qualche non allineamento concettuale o linguistico, e offrire una visione di più di due particelle/sistemi giuridici che lavorano insieme.

⁷ The White House, *Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy*, Washington D.C., 2012, p. 31 *et seq.*

⁸ Torben Holvad, “Mutual recognition, standards and interoperability”, in Matthias Finger e Pierre Messulam, *Rail economics, regulation and policy in Europe*, Cheltenham, Edward Elgar Publishing, 2015, pp. 275-302, p. 280:

«The principle of mutual recognition is fundamental to the functioning of the EU Single Market and the free movement of goods within the European Union. It establishes that: Member States must allow a product that has been lawfully produced and marketed in another Member State into their own market. This is the case even if the product does not comply with the technical rules in that country. The mutual recognition principle can only be disregarded by a Member State in case of overriding general interest, such as that relating to public health or environmental protection [...]».

Tuttavia, nel contesto dell'UE, trasferire dati personali senza contare su standard normativi armonizzati potrebbe infrangere le garanzie stabilite nella legislazione dell'Unione sulla protezione dei dati personali che richiede generalmente a un Paese terzo o ad un'organizzazione internazionale di applicare un livello di protezione "equivalente" a quello dell'Unione. Il diritto umano alla "*privacy*", nelle sue molteplici concettualizzazioni, e il diritto fondamentale alla protezione dei dati personali consacrato per la prima volta nell'art. 8 della Carta dei Diritti Fondamentali dell'UE⁹ (CDFUE), potrebbero essere pregiudicati quando la messa a disposizione dell'informazione dell'individuo costituisce un'ingerenza sproporzionata. Dopo lo scandalo Snowden¹⁰, sistemi giuridici che si consideravano "vicini" al modello europeo sono guardati con diffidenza visto che sono stati giudicati incompatibili con la scala di valori dell'Unione. Di conseguenza, la "interoperabilità globale" dovrebbe essere soppesata con cautela con i diritti garantiti a ciascun individuo.

Secondo l'art. 50 dei Regolamenti fratelli, la comunicazione dei dati personali a Paesi terzi, organizzazioni internazionali, e parti private è regolata dai regimi sul trasferimento di dati personali previsti dai sistemi IT su larga scala soggiacenti. Inoltre, i Regolamenti IO avanzano la conclusione di un Accordo di Cooperazione con l'Organizzazione Internazionale della Polizia Criminale (Interpol) che interconetterebbe l'interoperabilità con le banche dati di Interpol dei Documenti di Viaggio Rubati e Smarriti (SLTD) e dei Documenti di Viaggio Associati a Notifiche (TDAWN). Secondo questa norma:

«Fatti salvi l'articolo 65 del regolamento (UE) 2018/1240, gli articoli 25 e 26 del regolamento (UE) 2016/794, l'articolo 41 del regolamento (UE) 2017/2226, l'articolo 31 del regolamento (CE) n. 767/2008 e la consultazione delle banche dati Interpol attraverso l'ESP in conformità dell'articolo 9, paragrafo 5, del presente regolamento, che sono conformi alle disposizioni del capo V del regolamento (UE) 2018/1725 e del capo V del regolamento (UE) 2016/679, i dati personali conservati nelle componenti dell'interoperabilità o da queste trattati o consultati non sono trasferiti o messi a disposizione di paesi terzi, organizzazioni internazionali o soggetti privati».

I co-legislatori hanno presentato il quadro giuridico sull'interoperabilità come una soluzione efficace ed effettiva per raggiungere gli obiettivi dello SLSG. Di fatti, le regole sottostanti alla comunicazione dei dati personali richiamano quelle stabilite nell'*acquis* dell'Unione sulla protezione dei dati personali, ovvero: il capo V del trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione¹¹ (EUDPR);

⁹ Carta dei diritti fondamentali dell'Unione europea, GU C 326 del 26.10.2012, pp. 391-407.

¹⁰ Edward Snowden tradotto da Esther Cruz Santaella, *Vigilancia Permanente*, Barcellona, Planeta, 2019.

¹¹ Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la

il capo V del Regolamento generale sulla protezione dei dati¹² (GDPR), ed (eventualmente) il capo V della Direttiva sul trattamento dei dati personali per le forze di polizia¹³ (LED). Tuttavia, non è chiaro se ed in che termini la dimensione esterna dell'interoperabilità rispetta i parametri normativi stabiliti nel diritto internazionale e in quello dell'UE e, ci si chiede: l'interoperabilità rispetta, elude, o viola le regole e i principi applicati dall'UE nelle sue relazioni esterne sulla comunicazione dei dati personali a terzi?

1.2. Obiettivo e quesiti della ricerca

1.2.1. Obiettivo principale e quesito della ricerca ivi relazionato

L'obiettivo principale perseguito dalla presente ricerca è quello di determinare la portata esterna del quadro sull'interoperabilità stabilito dai Regolamenti (UE) 2019/817 e 2019/818, cioè, la loro estensione oltre le frontiere esterne dell'UE. Pertanto, questa tesi si propone di analizzare se l'interoperabilità dei sistemi centralizzati e le componenti dell'Unione con banche dati straniere è legale e “sostenibile” – i.e., coerente¹⁴ – rispetto alle regole e principi che regolano l'azione esterna dell'UE. Nello specifico, analizzeremo se l'art. 50 dei Regolamenti IO rispetta i quadri giuridici internazionali e sopranazionali e, nel caso, se i diritti delle persone, ovvero il diritto fondamentale alla protezione dei dati personali, sono realmente garantiti.

1.2.2. Domande ausiliari

Per rispondere alla domanda di ricerca principale, dobbiamo preliminarmente dare risposta alle seguenti questioni:

1. In che cosa consiste l'*acquis* dell'UE sulla protezione dei dati personali e come si applica allo SLSG?

decisione n. 1247/2002/CE (Testo rilevante ai fini del SEE.), PE/31/2018/REV/1, GU L 295 del 21.11.2018, pp. 39-98.

¹² Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (Testo rilevante ai fini del SEE), GU L 119 del 4.5.2016, pp. 1-88.

¹³ Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, GU L 119 del 4.5.2016, pp. 89-131.

¹⁴ Art. 7 della Versione consolidata del trattato sul funzionamento dell'Unione europea, GU C 326 del 26.10.2012, pp. 47-390 (TFUE): «L'Unione assicura la coerenza tra le sue varie politiche e azioni, tenendo conto dell'insieme dei suoi obiettivi e conformandosi al principio di attribuzione delle competenze».

2. Come si regola la protezione e il trasferimento dei dati personali nell'UE?
3. Qual è il ruolo che l'Agenzia dell'Unione Europea per la gestione operativa dei sistemi IT su larga scala nello Spazio di Libertà, Sicurezza e Giustizia (eu-LISA) ricopre davvero?
4. A parte l'interconnessione dei sistemi IT su larga scala, qual è la vera portata – i.e., circostanze, obiettivi, e contenuto – del quadro sull'interoperabilità?
5. Come si relaziona l'interoperabilità con la competenza esterna dell'UE sulla protezione dei dati personali e sulla libera circolazione di questi dati?

1.3. Ipotesi

Rispondendo al nostro quesito principale, ci aspettiamo di concludere che la portata esterna dell'interoperabilità assuma diverse sfumature. Prima di tutto, crediamo che la dimensione esterna dell'interoperabilità non debba essere ridotta ad una funzione meramente di supporto dei sistemi IT su larga scala e delle agenzie dell'UE involucrate, e che – a parte l'interconnessione con le banche dati di Interpol che è espressamente prevista – l'art. 50 dei Regolamenti IO stabilisce nuove forme e canali di comunicazione per lo scambio di dati personali con parti terze. Altrimenti, suddetta norma non apporterebbe nessun valore aggiunto rispetto alle regole sul trasferimento dei dati personali previste per i sistemi IT su larga scala coinvolti. Nello specifico, avanziamo l'ipotesi per la quale l'art. 50 dei Regolamenti IO permetterebbe l'interoperabilità tra le c.d. componenti e le banche dati di Paesi terzi e organizzazioni internazionali per rafforzare la capacità operativa dell'Unione nello SLSG, sia nella sua dimensione interna che in quella esterna. Questa supposizione ci impone di analizzare la portata interna dell'interoperabilità così come il suo valore aggiunto rispetto agli obiettivi perseguiti dai sistemi IT su larga scala coinvolti.

Di qui, proponiamo una seconda ipotesi di ricerca per la quale ci prospettiamo diversi gradi di interoperabilità in termini di interconnessione e di leggibilità dei dati. Questa tesi è corroborata alla luce di una definizione ampia di “trasferimento di dati personali” che include diversi meccanismi di messa a disposizione dei dati ad altre parti – e.g., lo «scambio di dati personali» o la «scoperta dei dati personali» –, e che dovrebbe considerare le peculiarità del regime di protezione dei dati personali nello SLSG. Di conseguenza, la nostra ricerca abbraccia un'interpretazione non letterale ma sistematica dell'art. 50. Prendendo in considerazione l'evoluzione tecnico-politica dei sistemi IT su larga scala degli ultimi vent'anni, dovremmo riscontrare che le agenzie dello SLSG con accesso all'architettura dell'interoperabilità – ovvero, l'Agenzia dell'Unione europea di Cooperazione di Polizia

(Europol), l'Agenzia dell'Unione europea per la Cooperazione in materia di Giustizia Penale (Eurojust), l'Agenzia Europea della Guardia di Frontiera e Costiera (Agenzia EGFC) e l'Agenzia dell'Unione europea per l'Asilo (EUAA) – possono accedere ai dati custoditi in modo centralizzato e condividerli mediante accordi amministrativi, vincolanti o meno, conclusi tra di loro o con Stati terzi e organizzazioni internazionali.

Questa premessa ci suggerisce che la legalità e sostenibilità di qualsiasi tipo di interoperabilità deve dedursi da uno studio caseo per caso alla luce dei principi e delle regole che governano l'azione esterna dell'UE in materia di protezione dei dati personali. La comunicazione dei dati personali, a istanza di una macchina o di un essere umano, deve rispettare il quadro legale sull'azione esterna dell'UE – o dei suoi organi –, il che comprende la CDFUE alla quale l'Unione è soggetta. Suddette garanzie non devono essere aggirate per il bene comune di un maggior ordine e sicurezza nello SLSG. Visto che il quadro sull'interoperabilità dovrebbe pesare più sui nazionali provenienti da Paesi terzi che sui cittadini dell'Unione, potrebbe essere necessario adottare delle garanzie ulteriori in grado di fronteggiare le situazioni di vulnerabilità e, nello specifico, di prevenire qualsiasi trattamento discriminante, restrittivo o repressivo. Crediamo quindi che, nella prassi, la protezione di alcuni gruppi di persone – e.g., bambini e richiedenti di asilo – è colpita in particolar modo.

A questo punto, la nostra ricerca sarebbe soddisfacente ma non completa: dobbiamo contemplare la possibilità che il quadro normativo dell'UE regolante la protezione dei dati personali e la libera circolazione di questi dati potrebbe essere modificato per sanare situazioni in cui i dati personali non sono debitamente protetti, così come le lacune legislative. Analizzare se l'art. 50 dell'interoperabilità rispetta l'*acquis* dell'UE potrebbe non essere sufficiente, e dobbiamo avanzare proposte *de lege ferenda* a seconda di come l'art. 50 bilanci la necessità di cooperare con terzi nell'ambito dello SLSG con la protezione transfrontaliera dei diritti fondamentali della persona.

2. Il “perché” della ricerca

Sin dalla fine degli anni '90, l'evoluzione sperimentata nel settore dell'IT ha trasformato la comunità internazionale in un modo globalizzato ed interconnesso. Il diffondersi ed il miglioramento della tecnologia della computazione e dell'intelligenza artificiale (AI), che promuovono questa rivoluzione grazie alla valanga di informazioni che diffondiamo quotidianamente¹⁵, sollevano dubbi sulla loro compatibilità rispetto alla protezione dei diritti

¹⁵ Joint Research Centre Technical Report, *AI Watch: Beyond pilots: sustainable implementation of AI in public services*, Lussemburgo, 2021, p. 32 et seq.: «One of the most fundamental requirements of AI is data. By

umani. Come sottolinea il Garante Europeo sulla Protezione Dati (GEPD), le tecnologie dell'informazione e della comunicazione (TIC) costituiscono una nuova sfida per la sfera privata della persona, poiché i dati personali sono trattati in forme diverse – raccolti, ordinati, filtrati, trasferiti o conservati in altro modo – il che moltiplica i rischi di ingerenza¹⁶.

I Regolamenti IO si collocano tra le riforme più recenti intraprese dall'Unione per salvaguardare in modo efficiente lo spazio di libertà di movimento che ha dovuto affrontare numerose crisi. Le continue minacce che si sono scontrate contro l'area Schengen hanno portato all'introduzione del quadro dell'interoperabilità ancora prima che la Commissaria Von Der Leyen lanciasse la Strategia Digitale dell'UE, il 9 maggio 2021¹⁷. Ci chiediamo, quindi, se una riforma così invasiva sia stata adottata con sufficiente cautela e consapevolezza o se il legislatore abbia, si passi il termine, usato la crisi umanitaria per promuovere un quadro giuridico restrittivo dei diritti fondamentali di ogni individuo – soprattutto delle persone migranti.

La risoluzione di “vecchi problemi” con meccanismi innovativi sta fomentando la realizzazione di nuovi progetti di ricerca che si chiedono se il nuovo contesto digitale assicuri adeguatamente la protezione dei diritti umani. Dopo l'11-S, i programmi di stoccaggio di dati *collect it all* – “colleziona tutto” – degli Stati Uniti (US) dimostrò che la vigilanza *cyber* può restringere in modo sproporzionato il diritto umano alla riservatezza e, a livello sopranazionale, il diritto alla protezione dei dati personali sotto il pretesto di voler contrastare criminali e terroristi. Da quel momento in poi, un clima di sfiducia nei confronti dei servizi di intelligence si è riversato in tutto il mondo, ostacolando il flusso di dati transnazionale che è divenuto un argomento molto sensibile. Il fatto che il nuovo quadro

definition, AI relies on access being ensured to the “right” kind of data on which to perform its analyses, and which in most cases is augmented by the results of the analyses themselves. For many Public Sector organizations though, fulfilling this requirement is a challenge, due to **a variety of obstacles in obtaining data of the quality and format they require**». Il Parere Preliminare del GEPD, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, Bruxelles, 10.03.2014, p. 9, riferisce che ogni giorno vengono raccolti e combinati 2,3 trilioni di gigabyte di dati per generare servizi e mappature globali.

¹⁶ Si vedano: il Parere del GEPD sulla *Promoting Trust in the Information Society by Fostering Data Protection and Privacy*, Bruxelles, 18.03.2010; la Sintesi del parere del Garante europeo della protezione dei dati sulla comunicazione della Commissione «Agenda digitale per l'Europa — Le tecnologie digitali come motore della crescita europea», *GU C 358* del 7.12.2013, pp. 17-18, e la Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni *Proteggere le infrastrutture critiche informatizzate - “Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai ciberattacchi e dalle ciberperturbazioni”* {SEC(2009)399} {SEC(2009)400}, COM(2009) 149 definitivo, Bruxelles, 30.3.2009.

¹⁷ La strategia è disponibile sulla pagina web ufficiale della Commissione europea al seguente link www.ec.europa.eu. Si noti che «a Europe fit for the digital age» è uno degli obiettivi politici chiave concordati nella Joint Declaration of the European Parliament, the Council of the European Union and the European Commission, *EU Legislative Priorities for 2022*, Bruxelles, 2022.

sull'interoperabilità stabilito dai Regolamenti (UE) 2019/817 e 2019/818 permetta ai dati personali di fuoriuscire dall'Unione verso terzi, mette in discussione la validità e opportunità di una forma di "interoperabilità globale" illimitata. Inoltre, si deve tener conto di altri principi inderogabili – e.g., la proibizione di discriminazione e il *non-refoulement* – nel caso in cui fossero coinvolti gruppi di migranti vulnerabili.

2.1. Studi previ

Premesso che un primo tentativo di stabilire un quadro sull'interoperabilità all'interno dello SLSG risale al periodo successivo all'11-S, diversi studi correlati al nostro tema di ricerca sono stati condotti a partire dagli anni 2000. Concretamente, si possono riconoscere due correnti culturali:

- un primo gruppo di studi si concentra sull'interoperabilità tra il SIS, il VIS e l'Eurodac, anche se questo progetto è stato scartato a causa di problemi legali, politici e tecnici;
- un secondo gruppo di lavori è stato proposto in seguito alla Comunicazione della Commissione europea su Sistemi d'Informazione più Forti e più Intelligenti per le Frontiere e la Sicurezza adottata il 6 aprile 2016¹⁸ e riguarda i Regolamenti IO o, più in generale, i sistemi IT su larga scala.

In entrambi i casi, la scuola belga guidata dal Prof. De Hert è stata pioniera nell'avanzare studi sull'interoperabilità all'interno dello SLSG, ed è stata poi affiancata, ad esempio, dalla scuola francese del Prof. Bigo, dalla scuola olandese della Prof.ssa Brouwer e, più recentemente, da quella londinese della Prof.ssa Vavoula. Si prevede che quest'ultima pubblicherà un'importante monografia sui sistemi IT su larga scala poco dopo la presentazione della nostra tesi.

2.2. Situazione attuale

Tutti i contributi sul quadro normativo dell'interoperabilità stabilito dai Regolamenti (UE) 2019/817 e 2019/818 adottano un unico approccio normativo, interno: quello dei diritti umani. Innanzitutto, l'interoperabilità e i suoi sistemi IT su larga scala sono analizzati rispetto alla protezione del diritto individuale alla riservatezza e, ancor più importante, il diritto fondamentale alla protezione dei dati personali previsto dalla CDFUE. Altri studi, invece, analizzano l'impatto dei Regolamenti fratelli sull'individuo tenendo in

¹⁸ Comunicazione della Commissione al Parlamento Europeo e al Consiglio, Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza, COM(2016) 205 final, Bruxelles, 6.4.2016.

considerazione che i dati personali che lo riguardano potrebbero essere trattati dalle agenzie dell'Unione invece che dalle autorità nazionali. Questi contributi apportano solo risultati parziali sul quadro giuridico dell'interoperabilità e, in alcuni casi, inducono a errore a causa della mancanza di un'analisi olistica. In sintesi, l'interoperabilità è stata analizzata prendendo in considerazione un punto di vista disciplinare specifico e non esiste una teoria omnicomprensiva sulla dimensione esterna dei Regolamenti (UE) 2019/817 e 2019/818. Ciononostante, questi studi sono estremamente utili: costatano che al quadro dell'interoperabilità si applicano diverse teorie, e che numerose altre teorie devono essere prese in considerazione quando analizziamo la sua dimensione esterna. Il quadro giuridico risultante, sebbene complesso, fa sì che il nostro lavoro sia il più originale possibile.

3. Il “come” della ricerca

3.1. Quadro giuridico

Il fondamento ultimo della presente tesi poggia sul liberalismo e l'umanesimo nel contesto di un'organizzazione internazionale mirata – cioè l'UE – basata sul rispetto dei diritti umani, delle libertà individuali, della diversità, della solidarietà e della democrazia¹⁹. Come afferma il Prof. Liñán Noguerras, l'UE gode di una personalità giuridica derivata, condizionata dalla volontà dei suoi Stati membri, e limitata nella sua portata e nel suo contenuto, che sono determinati dalle sue funzioni²⁰. La configurazione di un ordinamento giuridico sopranazionale, che procede verso la più stretta integrazione possibile tra i suoi Stati membri, ha permesso lo sviluppo di un quadro giuridico che assicura «un alto livello di protezione» dei dati personali, senza precedenti, anche in Materia di Cooperazione di Polizia e Giudiziaria Penale (PJCCM). La *leadership* digitale dell'UE prende le mosse da una nuova competenza che le è stata conferita nel 2007 per regolare la protezione dei dati personali e la libera circolazione di questi dati, ovvero l'art. 16 del TFUE. Questa nuova competenza stabilisce un legame diretto con il diritto fondamentale alla protezione dei dati personali e il diritto alla riservatezza ex arts. 8 e 7 della CDFUE, la quale è vincolante dal 2009.

¹⁹ Art. 2 della versione consolidata del trattato sull'Unione europea, GU C 326 del 26.10.2012, pp. 13-390 (TUE).

²⁰ Si veda Diego Javier Liñán Noguerras, “La acción de la Unión: las relaciones exteriores (I)”, in Araceli Mangas Martín e Diego Javier Liñán Noguerras, *Instituciones y Derecho de la Unión Europea*, Madrid, Tecnos, 2020, risorsa on-line.

Tuttavia, il filo conduttore della nostra ricerca non giace solo nell'*acquis* interno dell'UE basto sull'art. 16(2) TFUE, ma anche sui principi e le regole che l'UE deve rispettare come attore globale soggetto al diritto internazionale pubblico quando agisce esternamente²¹. Di conseguenza, la dimensione esterna dei Regolamenti IO deve essere analizzata con un approccio basato sulle competenze alla luce del regime di trasferimento dei dati personali del RGPD, della LED, e del EUDPR. Nello specifico, dovremmo far riferimento alle teorie delle relazioni esterne delle organizzazioni internazionali, e nella specie dell'UE. In virtù della giurisprudenza *AETR/ERTA*²² della Corte di Giustizia dell'UE (CGUE), l'Unione può acquisire una competenza esterna (implicita) per garantire che gli standard continentali non vengano elusi nel caso in cui i dati personali vengano trasferiti ad autorità straniere. L'UE è stata la prima organizzazione ad adottare un modello di "adeguatezza" o "basato sulla geografia" che autorizza la Commissione europea a valutare le legislazioni di parti terze sulla base di quella dell'UE. Secondo questo regime, l'adozione di una decisione di adeguatezza dovrebbe essere preferita alla conclusione di un trattato internazionale così come alle clausole che derogano al regime generale. Nel *Parere 1/15*²³, la CGUE ha chiarito che il trasferimento di dati personali, noti come *Passenger Name Record* (PNR), a un Paese terzo dovrebbe essere sigillato in un accordo internazionale fondato su entrambi gli artt. 87(2)(a) e 16(2) del TFUE, che coprono le misure riguardanti il trasferimento di dati personali e la protezione di tali dati, rispettivamente. Supponendo che l'insieme delle norme sulla protezione dei dati personali che regolano il loro trasferimento possa costituire esercizio della competenza dell'UE sulla protezione dei dati personali e sulla libera circolazione di tali dati in base all'art. 16(2) del TFUE, si contribuirà a chiarire la dicotomia esistente tra decisione di adeguatezza e accordo internazionale.

In realtà, questo quadro giuridico si applica sia quando l'Unione agisce direttamente sia quando delega l'esecuzione delle sue competenze a organizzazioni esterne e organismi interni. Dato che il secondo livello della dimensione esterna dell'interoperabilità si strutturerà sulla base delle agenzie dell'Unione che hanno accesso alla nuova infrastruttura informatica, la nostra ricerca si erige su una seconda teoria principale, cioè quella della delega. In

²¹ Al contrario, la nostra ricerca non si occupa dei quadri internazionali e sopranazionali sulla cybersicurezza, poiché il secondo protocollo aggiuntivo alla Convenzione sulla criminalità informatica sulla cooperazione rafforzata e la divulgazione di prove elettroniche, firmato a Strasburgo il 12 maggio 2022, e la strategia dell'UE sulla criminalità informatica erano ancora in fase di revisione.

²² C-22/70, *Commissione delle Comunità europee contro Consiglio delle Comunità europee. Accordo europeo trasporti su strada*, 31 marzo 1971, EU:C:1971:32.

²³ *Parer 1/15*, 26 luglio 2017, EU:C:2017:592.

particolare, la sentenza *Meroni*²⁴ e la giurisprudenza successiva ivi correlata completano la teoria sulle competenze esterne implicite quando l'Unione delega alle sue agenzie la conclusione di accordi e intese amministrative poiché, per raggiungere gli obiettivi interni assegnati, è necessaria la cooperazione con le autorità straniere. La teoria sulle relazioni esterne dell'UE si basa sul principio fondamentale del conferimento di competenze che impone all'UE, così come alle sue istituzioni, di agire entro i limiti stabiliti dai Trattati istitutivi – cioè, una base giuridica esplicita stabilita nei Trattati istitutivi e che conferisce il potere all'UE di agire all'esterno o, in assenza di una disposizione esplicita, la sua attribuzione mediante la teoria delle competenze implicite²⁵. La dottrina *Meroni* (rivista) impone alla cosiddetta autorità “principale” di “far scivolare la sua responsabilità”²⁶ all'organismo delegato affinché si possa affermare che sussiste effettivamente una delega di competenze. L'azione esterna delle agenzie dell'Unione è limitata ai cosiddetti accordi o intese “tecnico-amministrative”, essendo la loro attuazione conclusa alla luce dell'art. 218 TFUE o, in generale, come esecuzione della legislazione dell'UE. Come ha ricordato l'Avvocato generale Tesauro:

«[...] il diritto internazionale conosce gli accordi vincolanti e - a voler tutto concedere - la singolare categoria degli accordi non vincolanti, qualificati in modo vario e colorito, ma che possono ricondursi essenzialmente a due ipotesi: "gentlemen' s agreements", che talvolta possono rivestire un alto valore politico ed essere addirittura assistiti da un meccanismo di controllo internazionale quanto alla loro osservanza, oppure "intese" destinate a consolidare degli orientamenti, delle linee di condotta in determinati settori, ma sfornite di qualsivoglia valore giuridico, come peraltro risulta spesso dalla esplicita volontà delle parti. Né mi sembra superfluo, al riguardo, sottolineare che tali accordi sono in ogni caso normalmente conclusi dalle autorità competenti a stipulare e non da qualsiasi altra autorità o istituzione»²⁷.

Tuttavia, autorizzare le agenzie in materia di libertà, sicurezza e giustizia a comunicare dati personali a terzi attraverso strumenti amministrativi, come prevede il EUDPR, non deve oltrepassare il mandato operativo di ogni agenzia, e non deve infrangere i limiti stabiliti dalla giurisprudenza post-*Meroni*.

²⁴ C-9/56, *Meroni & Co., Industrie Metallurgiche S.p.A. contro l'Alta Autorità della Comunità europea del Carbone e dell'Acciaio*, 13 giugno 1958, EU:C:1958:7.

²⁵ Jacopo Alberti, *Le Agenzie dell'Unione Europea*, Milano, Giuffrè, 2018, p. 33 et seq., p. 419: «[...] le agenzie i cui regolamenti istitutivi non prevedono la competenza ad agire a livello internazionale non sono sempre esentate dal farlo [...]».

²⁶ Renaud Dehousse, “Delegation of Powers in the European Union: The Need for a Multi-Principals Model”, *West European Politics*, Vol. 31, No. 4, 2008, pp. 789-805.

²⁷ Conclusioni dell'Avvocato generale Tesauro, C-327/91, *Repubblica francese contro Commissione delle Comunità europee*, 16 dicembre 1993, EU:C:1993:941, para. 22. Vedi anche C-66/13, *Green Network Spa v Autorità per l'energia elettrica e il gas*, 26 novembre 2014, EU:C:2014:2399, che estende l'effetto *AETR/ERTA* agli accordi conclusi dagli Stati membri e dalle autorità amministrative dei Paesi terzi, e Florin Coman-Kund, “EU agencies as global actors: a legal assessment of Europol's international dimension”, *Maastricht Faculty of Law Working Paper*, No. 6, 2014, pp. 1-43.

3.2. Metodo

Il metodo utilizzato nella presente ricerca segue l'approccio disciplinare della dogmatica giuridica, o scienza giuridica. Si utilizzano diverse tecniche ermeneutiche: il metodo abduttivo ci aiuta a ispezionare l'effettiva portata dei Regolamenti IO sia internamente che esternamente; il ragionamento analitico, o deduttivo, è indispensabile per valutare la coerenza dell'art. 50 dei Regolamenti IO con il quadro generale del RGPD, della LED e del EUDPR; il metodo induttivo, invece, è utile per dedurre che i Regolamenti IO perseguono un nuovo modello di identità o di gestione dei casi, per esempio.

La tesi si basa su risorse primarie raccolte nel periodo 2019-2022. Alcune risorse primarie sono state elaborate attraverso un approccio quantitativo e contemplano: in primo luogo, interviste strutturate e semi-strutturate condotte tra il 2020 e il 2022; in secondo luogo, le conoscenze empiriche della dottoranda acquisite durante il suo periodo di ricerca presso la Commissione europea. Diverse indagini sono state realizzate a Bruxelles, principalmente online a causa del COVID-19, a:

- sette funzionari della Direzione Generale della Migrazione e degli Affari Interni (DG HOME) che si occupano dell'attuazione della riforma dell'interoperabilità, dei sistemi IT su larga scala, della falsificazione o del furto di documenti e del rimpatrio di cittadini di Paesi terzi;
- un funzionario della Rete europea per il ritorno e il reinserimento (ERRIN);
- un funzionario dell'Agenzia EGFC;
- un funzionario di Europol, e
- un funzionario di eu-LISA.

Inoltre, abbiamo realizzato un questionario sull'interoperabilità e lo abbiamo sottoposto al massimo esperto della DG HOME nel nostro ambito di ricerca. Il materiale empirico è stato elaborato durante il periodo di ricerca svolto presso la Commissione europea, nell'unità DG HOME-B3, da febbraio 2020 a febbraio 2021. Concretamente, la dottoranda ha svolto i seguenti compiti:

- supporto legale sull'interpretazione dei Regolamenti (UE) 2019/817 e 2019/818 e dei sistemi IT su larga scala correlati;
- redazione giuridica della legislazione secondaria a seguito dei Regolamenti (UE) 2019/817 e 2019/818;

- segnalazione di incontri con diverse parti interessate (Consiglio dell'UE, Stati membri, agenzie dell'Unione, Comitato dell'interoperabilità, Gruppo di esperti dell'interoperabilità, Gruppo consultivo eu-LISA, e così via);
- preparazione dei materiali di formazione, come documenti e presentazioni, e
- stesura del Manuale sull'interoperabilità.

Altre fonti primarie utilizzate includono: la letteratura (libri, tesi, riviste scientifiche *peer-reviewed*, riviste, rapporti e documenti); le leggi internazionali, sovranazionali e nazionali (principi e regole di diritto positivo) così come la giurisprudenza e i documenti ufficiali di *soft law*. Le informazioni sono state ricercate attraverso l'uso di parole chiave secondo i seguenti macro-campi di studio: diritti umani; *privacy* e protezione dei dati; relazioni esterne dell'UE; SLSG; agenzie dell'Unione; sistemi IT su larga scala e interoperabilità. Queste risorse sono state analizzate con un approccio qualitativo che garantisce una visione olistica dei problemi giuridici presentati nel nostro oggetto di ricerca.

Le fonti secondarie sono integrate dalle banche dati giuridiche dell'Università di Granada (Spagna), l'Università di Ferrara (Italia), la Biblioteca della Commissione europea (Belgio), e la Biblioteca del Palazzo della Pace (Olanda). Sono state consultate anche piattaforme *open-source* – per esempio, Dialnet e Google Accademico – e siti web pubblici – per esempio, ec.europa.eu, consilium.europa.eu, europarl.europa.eu.

3.3. Contenuto

La tesi si sviluppa in sei capitoli. I primi due Capitoli si concentrano sulla competenza normativa dell'UE sulla protezione dei dati personali e sulla libera circolazione di questi dati incorporata nell'art. 16 TFUE e il diritto fondamentale corrispondente alla protezione dei dati personali consacrato nell'art. 8 della CDFUE. L'analisi si basa sul sistema di competenza dell'UE sorretto dal principio di attribuzione e sul presupposto che questo principio rappresenta la pietra miliare sulla quale qualsiasi organizzazione internazionale regola la sua azione interna ed esterna. Ciò risulta particolarmente rilevante per l'UE, dove la protezione dei diritti fondamentali è relegata all'implementazione delle politiche dell'Unione solamente. In questa fase preliminare, analizzeremo i principi sui quali si fonda l'*acquis* dell'UE sulla protezione dei dati personali e se questi si applicano all'intero SLSG. Di fatti, l'adozione della LED per PJCCM suggerisce che questo *acquis* subisce un'applicazione settoriale che introduce importanti deroghe a favore della prevenzione, investigazione, rilevamento, o prosecuzione dei delitti criminali o l'esecuzione delle condanne penali. In questo caso, diversi regimi sul trasferimento dei dati personali

potrebbero coesistere dipendendo della finalità del trattamento. La comunicazione dei dati personali a terzi è regolata da un quadro giuridico complesso che è fatto di norme e principi che modulano l'azione esterna dell'UE basata sull'art. 16 TFUE, anche quando questa base giuridica sia richiamata implicitamente dalle distinte forme di cooperazione dello SLSCG. Di conseguenza, la nostra ricerca non si limiterà ad analizzare le disposizioni che regolano il trasferimento dei dati personali alla luce della legislazione interna dell'UE, che già di per sé stabilisce un insieme di principi da rispettare per il trattamento di dati personali, ma si estende anche al quadro giuridico applicabile all'attività esterna dell'UE in quanto attore globale.

I Capitoli terzo e quarto analizzano l'evoluzione dei sei sistemi IT su larga scala che integrano l'infrastruttura dell'interoperabilità sino alla loro istituzionalizzazione in conformità con la dottrina della delega di poteri formulata dalla CGUE. I sistemi IT su larga scala sono stati implementati in conformità con politiche specifiche dello SLSCG ma rischiano di confondersi tra di loro nel quadro dell'interoperabilità. La loro esecuzione risponde al principio di attribuzione che richiede all'Unione di rispettare i limiti orizzontali stabiliti dai Trattati istitutivi. Tuttavia, ai dati personali conservati in modo centralizzato possono accedervi facilmente molteplici autorità e funzionari dell'Unione che perseguono altri obiettivi e rispondono ad un'altra competenza attribuita all'Unione. L'accesso non-controllato ai dati personali conservati nei sistemi IT su larga scala può dirsi incompatibile con i principi che regolano il trattamento dei dati personali, tra i quali risalta il principio della limitazione del trattamento alla prima finalità. Non è chiaro come suddetto approccio in materia di competenza si relazioni con quello adottato dalla normativa dell'Unione in materia di protezione dei dati personali, e se la loro compresenza ha contribuito all'adozione dei Regolamenti IO.

Ipotizziamo che il principio della limitazione del trattamento alla prima finalità abbia via via indebolito i limiti imposti alle politiche dell'Unione dai Trattati istitutivi, come testimonia il mandato di eu-LISA. Le agenzie dell'Unione permettono l'implementazione di competenze concorrenti grazie alla cooperazione tra funzionari dell'UE e le autorità nazionali degli Stati membri per evitare l'accentramento del potere esecutivo nelle mani della Commissione europea. Di conseguenza, l'istituzionalizzazione della competenza operativa dell'Unione per la gestione dei sistemi IT su larga scala potrebbe essere stato un passo fondamentale per sbloccare la riforma sull'interoperabilità dapprima proposta dopo l'11-S. Nel caso in cui eu-LISA fosse delegata competenze di sviluppo, implementazione, e monitoraggio dell'infrastruttura dell'interoperabilità, questa deve rispettare la

giurisprudenza *Meroni* rivisitata che ha definito i limiti alla delega di competenze dall'Unione ad altri organi. Al momento, non è chiaro se questa nuova agenzia ha accesso ai dati personali e, pertanto, se è competente per trasferire dati personali a Paesi terzi e organizzazioni internazionali.

I Capitoli quinto e sesto ispezionano le circostanze, il contenuto, e gli obiettivi dei Regolamenti IO e la loro portata esterna. Prima di analizzare la loro dimensione esterna, le circostanze, il contenuto e gli obiettivi dei Regolamenti fratelli sono esplorati per risaltare se i Regolamenti IO apportano un valore aggiunto ai sistemi sottostanti. I Regolamenti (UE) 2019/817 e 2019/818 prevedono quattro componenti che serviranno per raggiungere gli obiettivi dell'interoperabilità. Queste componenti sono: un portale di ricerca europeo (ESP); un servizio comune di confronto biometrico (BMS comune); un archivio comune di dati di identità (CIR), e un rilevatore di identità multiple (MID). Inoltre, i Regolamenti prevedono che si adotterà un archivio centrale di relazioni e statistiche (CRRS). Riteniamo che l'interoperabilità sia fornita di una serie di obiettivi propri che arricchiscono quelli perseguiti dai singoli sistemi. Di conseguenza, l'analisi della portata interna è indispensabile per capire come la nuova architettura possa facilitare l'interconnessione con banche dati straniere, come analizzeremo nell'ultimo Capitolo. L'art. 50 sarà analizzato tenendo conto del fatto che: innanzitutto, esistono diversi gradi di interoperabilità a seconda del fondamento giuridico sul quale si trasferiscono i dati personali; secondo, che le autorità nazionali, i sistemi IT su larga scala e le agenzie dell'Unione possono trasferire dati personali a seconda che l'intervento umano sia necessario o meno. Quest'analisi chiarirà i termini nei quali l'interoperabilità con banche dati straniere è legale e coerente con i principi e le regole analizzate nei Capitoli precedenti. Tuttavia, non ci soffermeremo sulla comunicazione dei dati personali mediante le componenti dell'interoperabilità a soggetti privati – ad esempio, ai vettori aerei – poiché questo aspetto non è stato ancora completamente regolato dai legislatori.

4. Il “chi”, “quando”, e “dove” della ricerca

La tesi è stata elaborata da Francesca Tassinari nel periodo 2019-2022: il primo e il secondo anno sono stati destinati alla raccolta delle fonti bibliografiche; tra il 2020-2021 la dottoranda ha soggiornato e studiato a Bruxelles e a Ferrara; la fase di scrittura si è conclusa nella primavera del 2022. L'intera ricerca è stata finanziata dal Ministero spagnolo dell'Educazione, della Cultura e dello Sport, e dal Vice-Rettorato per la Ricerca e il

Trasferimento dell'Università di Granada. La Commissione europea ha coperto parte dei costi del periodo di ricerca a Bruxelles.

CHAPTER I

THE EUROPEAN UNION'S COMPETENCE ON THE PROTECTION OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA

Until ICTs demonstrated their ability to seriously breach the privacy of individuals there had been very few discussions on the protection of personal data at the international level. The Council of Europe was the first international organisation to promote universal, binding principles on the protection of personal data processed in an automated manner with the adoption of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No 108 (Convention 108)¹. Following the adoption of Convention 108, Article 8 of the European Convention of Human Rights and Fundamental Freedoms² (ECHR) has been re-interpreted in the light of the contemporary digital environment. The EU, for its part, was pioneering in splitting the right to 'privacy' into a new right specifically directed at protecting personal data by virtue of Articles 7 and 8 of the CFREU. The 2007 Lisbon Treaty³ brought significant additions to the EU's powers by conferring upon it the competence⁴ to adopt measures on the protection of personal data and the free movement of such data under Articles 16 TFEU.

As the European Data Protection Supervisor (EDPS) states, the linkage between Article 16(1) TFEU and the fundamental right to the protection of personal data foreseen in Article 8 of the CFREU, ensures that the co-legislators are called on to provide effective protection, long-term legal frameworks, safeguard the right to the protection of personal data regardless of political influence, and only limits the individuals' rights in exceptional circumstances⁵. Read in conjunction, Article 16 TFEU and Article 8 CFREU form a core of principles that

¹ See the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *ETS* 108, signed in Strasbourg on 28 January 1981, entered into force on 1 October 1985.

² European Convention on Human Rights, *CETS* 005, signed in Rome on 4 November 1950, entered into force on 3 September 1953.

³ Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed in Lisbon on 13 December 2007, *OJ C* 306, 17.12.2007, pp. 1-271.

⁴ By virtue of the principle of conferral, Member States divest themselves from their powers and endorse the management of certain collective interests to an international organisation. From a technical-legal perspective, the act of conferral limits the powers of the organisation with respect to specifically affected matters in view of the achievement of pre-established goals. See Geert De Baere, *Constitutional Principles of EU External Relations*, Oxford, Studies in European Law, 2008, p. 19.

⁵ See the Opinion of the EDPS on *the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"*, Brussels, 4.01.2011, para. 30.

protect personal data according to the interpretation given by the CJEU⁶. Such a linkage impacts the exercise of the EU competence regarding the protection of personal data and the free movement of such data that must be systematised as an EU shared⁷ competence by default⁸. Provided that the EU legislates together with its Member States in the exercise of this new competence, the principles of subsidiarity, necessity, and proportionality can be revisited with an individual-centric interpretation. The latter, specifically, turns out to be of paramount importance in the light of the constraints EU law must respect by virtue of Article 52(1) of the CFREU⁹.

Article 16 TFEU has been strategically inserted within the provisions of general application that crosscut the founding Treaties, with the sole exception of the Common Foreign and Security Policy (CFSP), for which a specific provision is defined¹⁰. In the Action Plan implementing the Stockholm Programme of 2012, the European Commission stressed that Article 16 of the TFEU constitutes the new legal basis ‘[...] for a modernized and comprehensive approach to data protection and the free movement of personal data, also covering police and judicial cooperation in criminal matters’¹¹. The abolishment of the Greek template structure enabled the EU to extend its data protection *acquis* to areas previously

⁶ With the acronym CJEU we will refer also to the Court of Justice of the European Communities based on the Treaty establishing the European Economic Community, signed in Rome on 25 March 1957, entered into force on 1 January 1958 – Article 164 ff. – since this was substituted by the former with the Lisbon Treaty.

⁷ Araceli Mangas Martín, “Las competencias de la Unión Europea”, in Araceli Mangas Martín and Diego Javier Liñán Nogueras, 2020, *loc. cit.*, suggests speaking of “concurrent competences” instead of shared ones. She warns that the concept of concurrent shall not be assimilated to the one used in the US Constitution, being the latter comparable to what it is known as “parallel” competences within the EU legal order. However, we believe that the concept of “concurrent” may lead to misinterpretation since Article 4 TFEU is differently translated as ‘shared’ in English, ‘partagée’ in French, ‘concorrente’ in Italian, and ‘compartida’ in Spanish. Sticking to the English version, we would rather opt for the ‘shared’ expression instead the one of ‘concurrent’.

⁸ Article 4(1) TFEU consecrates the principle *in dubio pro concurrentia* as analysed by José Martín y Pérez de Nanclares, *El Sistema de competencias de la Comunidad Europea*, Madrid, McGraw-Hill, 1997, p. 156.

⁹ Article 52(1) CFREU: ‘Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others’.

¹⁰ Article 39 of the TEU: ‘In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities’.

¹¹ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century, COM(2012) 9 final, Brussels, 25.1.2012, p. 3. This approach recalls the European Commission’s Communications on The Stockholm Programme — an open and secure Europe serving and protecting citizens, OJ C115/1, Brussels, 4.5.2010, and the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Delivering an area of freedom, security and justice for Europe’s citizens: Action Plan Implementing the Stockholm Programme, COM(2010) 171 final, Brussels, 20.4.2010.

housed under an intergovernmental roof¹². Nevertheless, Declarations No 20 and No 21 of the Lisbon Treaty highlight that in the fields of PJCCM, as well as in national security matters, the EU shall exercise its competence in light of the objectives pursued therein without bypassing the Member States' national prerogatives¹³. In this sense, the AFSJ enriches the EU legislation on personal data through a specific spectrum of provisions directed at regulating the processing of personal data by competent authorities in charge of maintaining public order and security.

This Chapter analyses the EU's competence on the protection of personal data and its free movement with special emphasis on the AFSJ. First of all, Article 16 TFEU is presented as a supranational competence the regulation of which originated not from the Member States' constitutional traditions, but from the general principles of human rights law, taking the Council of Europe as the leading point of reference. Following this, the introduction of a Community's first Directive is presented as a piece of bottom-down legislation imposed on Member States that had not legislated on the issue yet, or had made little progress. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data¹⁴ (DPD) laid out a series of guarantees that were gathered under Article 8 of the CFREU on which basis the Court of Luxembourg tailors its jurisprudence consistently with the nearby Court in Strasbourg. Article 16 TFEU is then analysed as a shared competence between the Member States and the EU, the exercise of which is impacted by the fact it struggles both the founding Treaty and the EU bill of rights. Specifically, this paper will highlight how the principles of subsidiarity, necessity, and proportionality are understood by the co-legislators in light of the CFREU rather than in favour of the principle of sovereignty. Finally, we will highlight how, despite its crosscutting position, Article 16 TFEU labours under sectorial applications as the AFSJ shows, which hampers the creation of comprehensive horizontal regulation on data protection. This Chapter aims to assess if the EU has been granted internal competence on the protection of personal data, what the nature of this competence is, and which features characterise and limit its application in the AFSJ.

¹² Current Chapters 4 and 5 of Title V of the TFEU.

¹³ Article 4(2) *in fine* of the TEU.

¹⁴ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ L* 281, 23.11.1995, pp. 31-50.

1. Reinterpreting the human right to privacy in the digital age

1.1. The United Nations' delayed, soft response to technology challenges

The IT revolution that started in the US in the '50s launched widespread discussions on the protection of the individual's rights *vis-à-vis* the automated processing of information through computer technology. Although several other rights were threatened due to the ease of storing and disseminating information, privacy laid at the centre of the debate. Increasingly associated with computer technologies¹⁵, the right to privacy¹⁶ was reinterpreted by Prof. Westin as aiming to keep control of how individual's data was used¹⁷.

At the time, existing human rights law and its instruments were deemed to be sufficiently flexible to offer protection to the individual, citizens, and foreigners¹⁸ in the face of potential misuse by ICTs. The International Bill of Human Rights¹⁹ adopted by the United Nations (UN) already considered the right to privacy – in French, *vie privée* – in Article 12 of the Universal Declaration of Human Rights (UDHR) of 10 December 1948²⁰, establishing that

¹⁵ Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Switzerland, Springer International Publishing, 2014, p. 29.

¹⁶ Colin J. Bennett and Rebecca Grant, *Visions of Privacy: Policy Choices for the Digital Age*, Toronto, University of Toronto Press, 1999, p. 77 ff., frame privacy in its traditional conception as associated to Big Brother, secrecy paradigm, and invasion conception.

¹⁷ Alan F. Westin, *Privacy and Freedom*, New York, Atheneum, 1970, p. 7: '(p)rivacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'. See also Austin Sarat, "Whither Privacy? An Introduction", in Austin Sarat, *A World Without Privacy: What Law can and Should Do?*, New York, Cambridge University Press, 2015, pp. 1-32, p. 16 ff., and Vanmala Hiranandani, "Privacy and security in the digital age: contemporary challenges and future directions", *The International Journal of Human Rights*, Vol. 15, No. 7, 2011, pp. 1091-1106.

¹⁸ Helena Torroja Mateu, "La «protección diplomática» de los «derechos humanos» de los nacionales en el extranjero: ¿situaciones jurídicas subjetivas en tensión?", *Revista Española de Derecho Internacional*, Vol. 58, No. 1, 2006, pp. 215-237, p. 218 (the translation is ours):

'The notion of human rights and fundamental freedoms of the human being without distinction on grounds of race, sex, language, religion or other grounds, contains behind it the idea of erasing the national/foreigner distinction as a criterion for recognising the rights of the individual in international law. From now on, the state will have international obligations to respect the human rights of all persons under its jurisdiction, whether they are nationals, foreigners, stateless persons...'

However, the author (p. 225) underlines that the concept of "essential human rights" substituting the one of "minimum standard of rights" has not been resolved and still it is unclear which rights have to be recognised to foreign nationals to comply with general international law and to *ius cogens* norms.

¹⁹ Frédéric Mégret and Philip Alston, *The United Nations and Human Rights: A critical appraisal*, Oxford, Oxford University Press, 2020; Isabel Hernández Gómez, *Sistemas internacionales de Derechos humanos*, Madrid, Dykinson, 2001, pp. 113-167; Philip Alston and Ryan Goodman, *International Human Rights. The successor to international human rights in context: law, politics and morals*, Oxford, Oxford University Press, 2013, pp. 685-761.

²⁰ Resolution of the UN General Assembly No. A/RES/217/(III) of 10 December 1948, *Universal Declaration of Human Rights*. Despite its soft character, the UDHR is a model to be followed by the international community and its dispositions have been bindingly interpreted to: first, authentically interpret the Charter of the UN signed in San Francisco on 26 June 1945, entered into force on 24 October 1945, available at www.un.org, that programmatically consecrates the promotion and encouragement of human rights within its

‘(n)o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation’²¹, as well as in Article 17 of the International Convention on Civil and Political Rights (ICCPR)²² that reiterated the latter point and added, in its second paragraph, that:

‘Everyone has the right to the protection of the law against such interference or attacks’²³.

objectives (Article 1(3)) and seals a general obligation for its members to effectively achieve ‘universal respect for, and observance of, human rights and fundamental freedoms’ (Articles 55 and 56); second, integrate the ‘general principles of law recognised by civilized nations’ – see Oriol Casanovas, *Compendio de Derecho Internacional Público*, Madrid, Tecnos, 2021, para. 404, and Juan Antonio Carrillo Salcedo, “Algunas reflexiones sobre el Valor Jurídico de la Declaración Universal de los Derechos Humanos”, in VV. AA., *Hacia un Nuevo Orden Internacional y Europeo: Homenaje al Profesor Manuel Díez de Velasco*, Madrid, Tecnos, 1993, pp. 167-178. Although some of the rights and freedoms consecrated therein have acquired customary nature, this is not the case of the right to privacy that lays out from the catalogue of “fundamental human rights” whose absolute character prohibits any kind of derogation – see Jaime Orúa Oraá, “The Declaration of Human Rights”, in Felipe Gómez Isa and Koen de Feyter, *International Human Rights Law in a Global Context*, Bilbao, HumanitarianNet, 2009, pp. 163-236, and Id., “En torno al valor jurídico de la Declaración Universal”, in VV. AA., *La Declaración Universal de Derechos Humanos en su cincuenta aniversario: Un estudio interdisciplinar*, Deusto, Instituto de Derechos Humanos, 1999, pp. 179-202.

²¹ Olivier De Schutter, *International Human Rights Law*, Cambridge, Cambridge University Press, 2017, p. 66 ff.; Jaime Orúa Oraá, 2009, *op. cit.*, p. 233; Richard B. Lillich, “Duties of States Regarding the Civil Rights of Aliens”, *Collected Courses of the Hague Academy of International Law*, Vol. 161, 1978, pp. 329-442; Theodor Meron, *International law in the Age of Human Rights: General Course on Public International Law*, Leiden/Boston, Martinus Nijhoff Publishers, 2003, pp. 9-490, and Oscar Schachter, “International Law in Theory and Practice General Course in Public International Law”, *Collected Courses of the Hague Academy of International Law*, Vol. 178, 1982, pp. 9-396. James Waldo, Herbert Lin, and Lynette I Millett, *Engaging privacy and information technology in a digital age*, Washington, National Academies Press, 2007, p. 1 ff., note:

‘[...] privacy is an ill-defined but apparently well-understood concept. It is ill-defined in the sense that people use the term to mean many different things. [...] privacy is a complicated concept that is difficult to define at a theoretical level under any single, logically consistent “umbrella” theory, even if there are tenuous threads connecting the diverse meanings. At the same time, the term “privacy” is apparently well understood in the sense that most people using the term believe that others share their particular definition. Nonetheless, privacy resists a clear, concise definition because it is experienced in a variety of social contexts’.

²² International Convention on Civil and Political Rights, *U.N.T.S.* Vol. 999, p. 171, and Vol. 1057, p. 407, signed in New York on 16 December 1966, entered into force on 23 March 1976 – all the Member States of the EU have ratified it according to the www.treaties.un.org – plus its Optional Protocol to the International Covenant on Civil and Political Rights, *U.N.T.S.* Vol. 999, p. 171, signed in New York on 16 December 1966, entered into force on 23 March 1976, and its Second Optional Protocol to the International Covenant on Civil and Political Rights, aiming at the abolition of the death penalty, *U.N.T.S.* Vol. 1642, p. 414, signed in New York on 15 December 1989, entered into force on 11 July 1991. Juan Antonio Carrillo Salcedo, *Soberanía de los estados y derechos humanos en derecho internacional contemporáneo*, Madrid, Tecnos, 2001, p. 74 ff., excludes the possibility that human rights treaties have promoted customary international norms (our own translation):

‘[...] despite the undeniable positive aspects of the numerous existing human rights treaties, in particular as regards the normative development of the provisions of the United Nations Charter relating to the dignity of the human person, the conventional network in question constitutes a *heterogeneous and highly diversified whole, and not a homogeneous legal continuum, both in terms of the number of States bound and bound by conventions and in terms of the scope and content of the obligations assumed by the States parties, which are not necessarily homogeneous or uniform*’.

²³ Read in conjunction with Article 2(1) of the ICCPR, Article 17 imposes on the contracting parties “positive obligations” to respect, protect, and fulfil (i.e., facilitate, provide, and promote) the rights consecrated therein – see Riccardo Pisillo Mazzeschi, “Responsabilité de l’État pour violation des obligations positives relatives aux droits de l’homme”, *Collected Courses of the Hague Academy of International Law*, Vol. 333, 2008, pp.

The Human Rights Committee must be given credit for firstly raising concerns regarding the respect and protection of the right to privacy²⁴ while other UN organs had been avoiding the issue²⁵ until the Edward Snowden scandal broke out²⁶. It was revealed that through the mass-surveillance programs Planning Tool for Resource Integration, Synchronisation, and Management (PRISM) and Upstream the US intelligence services had been eavesdropping on foreign citizens' private telecommunications in secret and on a vast scale. As a result, in 2013 the UN Human Rights Council²⁷ asked the UN High Commissioner for Human Rights²⁸ to create a report on the right to privacy in the digital area, which triggered a chain

187-506, p. 243. More controversial, instead, is the possibility to envisage an obligation to prevent, cease, and desist a breach of whatsoever human right rule upon other states than the perpetrator or over the whole international community – Hélène Raspail, “Due diligence et droits de l’homme”, in Sarah Cassella, *Le standard de due diligence et la responsabilité internationale*, Paris, Pedone, 2018, pp. 170-133, p. 127: ‘The notion of diligence appears to be diluted in the prevention of human rights violations, which takes on its autonomy and becomes a reinforced standard of state behaviour’ (our own translation). Article 4 of the ICCPR clarifies that the right to privacy has a relative character so that derogations are possible in the terms set forth therein. On the interpretation of Article 17 of the ICCPR see Matteo E. Bonfanti, “Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti”, *Diritti Umani e Diritto Internazionale*, Vol. 5, No. 3, 2011, pp. 437-481, p. 460, and Manfred Nowak, *The International Covenant on Civil and Political Rights*, Bilbao, HumanitarianNet, 2009, pp. 271-292.

²⁴ The General Comment No. 16 on Article 17 (Right to Privacy) of the Human Rights Committee of 8 April 1988, *The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, worried about the protection of the right to privacy before arbitrary interferences and illegalities perpetrated by public and private actors. On the Committee see Nisuke Ando, *Towards implementing Universal Human Rights*, Leiden/Boston, Martinus Nijhoff Publishers, 2004.

²⁵ In its plenary meeting No. 1748, the General Assembly adopted the Resolution No. A/RES/2450(XXIII) of 19 December 1968, *Human rights and scientific and technological developments*. Memorably was the Resolution of the Human Rights Council No. A/HRC/45/95 of 14 December 1990, *Guidelines for the regulation of computerized personal data files*, that established principles to personal data processed in informatic files.

²⁶ Edward Snowden translated by Esther Cruz Santaella, *loc. cit.*; Micheal Yilma Kinfe, “The Right to Privacy in the Digital Age: Boundaries of the New UN Discourse”, *Nordic Journal of International Law*, Vol. 87, No. 4, 2018, pp. 485-528; Carly Nyst and Tomaso Falchetta, “The Right to Privacy in the Digital Age”, *Journal of Human Rights Practice*, No. 9, 2017, pp. 104-118; Martin Weiler, “The Right to Privacy in the Digital Age: The Commitment to Human Rights Online”, *German Yearbook of International Law*, No. 57, 2014, pp. 651-666.

²⁷ The UN Human Rights Council promotes human rights through the Universal Periodic Review mechanism through which it scrutinises the human rights situation of contracting parties. It can receive individual's claims under two main procedures: first, it receives denounces of individuals and, eventually, it establishes an investigatory body without the state's affected consent; second, it receives individuals' communication on massive and flagrant violation of human rights which triggers a confidential proceeding with the state concerned. Since the '80s, the UN Human Rights Council – previously UN Human Rights Commission – has instituted a Special Rapporteurs system in charge of investigating a serious infringement on a specific theme – see, for example, José Antonio Pastor Ridruejo, *Curso de derecho internacional público y organizaciones internacionales*, Madrid, Tecnos, 2021, p. 221 ff.

²⁸ Resolution of the UN General Assembly No. A/RES/48/141 of 20 de December of 1993, *High Commissioner for the promotion and protection of all human rights*.

of resolutions adopted within the General Assembly²⁹, the Human Rights Council³⁰, and the High Commissioner for Human Rights³¹. The first report was presented on the occasion of the UN Human Rights Council's session No. 27 of 2014 and was specifically directed at addressing mass surveillance issues³². At the time, the concept of 'privacy' was fuzzily linked to a number of correlated human rights and freedoms – e.g., freedom of expression. Besides, the belief that Article 17 ICCPR was unenforceable left the community unsatisfied³³ especially in light of the Five Eyes (FVEY) alliance's³⁴ position of excluding any extraterritorial applicability³⁵ of the right to privacy with regard to foreign surveillance

²⁹ Resolutions of the UN General Assembly: No. A/RES/75/176 of 16 December 2020, *The right to privacy in the digital age*; No. A/RES/73/179 of 17 December 2018, *The right to privacy in the digital age*; No. A/RES/71/199 of 19 December 2016, *The right to privacy in the digital age*; No. A/RES/69/166 of 18 December 2014, *The right to privacy in the digital age*; No. A/RES/68/167 of 18 December 2013, *The right to privacy in the digital age*.

³⁰ Resolutions of the Human Rights Council: No. A/HRC/RES/48/4 of 13 October 2021, *Right to privacy in the digital age*; No. A/HRC/42/15 of 26 September 2019, *The right to privacy in the digital age*; No. A/HRC/38/7 of 5 July 2018, *Promotion, protection and enjoyment of human rights on the Internet*; No. A/HRC/37/2 of 22 March 2018, *The right to privacy in the digital age*; No. A/HRC/34/7 of 23 March 2017, *The right to privacy in the digital age*; No. A/HRC/32/13 of 1 July 2016, *The promotion, protection and enjoyment of human rights on the Internet*, and No. A/HRC/28/16 of 26 March 2015, *The right to privacy in the digital age*.

³¹ Resolution of the Human Rights Council: No. A/HRC/48/31 of 13 September 2021, *The right to privacy in the digital age. Report of the United Nations High Commissioner for Human Rights*; No. A/HRC/39/29 of 3 August 2018, *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights*, and No. A/HRC/27/37 of 30 June 2014, *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*.

³² Resolution of the Human Rights Council No. A/HRC/28/39 of 19 December 2014, *Summary of the Human Rights Council panel discussion on the right to privacy in the digital age*. On mass surveillances' concerns stemming from the processing of biometric data see, for example, the report for the GREENS/EFA of the European Parliament by Francesco Ragazzi, Elif Mendos Kuskonmaz, Ildikó Z Pájás, Ruben van de Ven, and Ben Wagner, *Biometric & Behavioural Mass Surveillance in EU Member States*, Brussels, 2021.

³³ Resolution of the Human Rights Council No. A/HRC/28/39 of 19 December 2014, para. 43:

‘Many observed, however, that the implementation of the right to privacy was lacking and that there was a need for concrete measures to safeguard that right. Some noted that unilateral and unauthorized access to private data and extensive surveillance needed to be addressed comprehensively and calls were made for urgent measures to be taken to stop current surveillance practices and protect individuals from violations of their right to privacy’.

³⁴ The alliance includes: US, United Kingdom, Australia, Canada and New Zealand. See Didier Bigo, “Beyond national security, the emergence of a digital reason of state(s) led by transnational guilds of sensitive information: the case of the Five Eyes Plus network”, in Ben Wagner, Matthias C. Kettmann, and Kilian Vieth, *Research handbook on human rights and digital technology: global politics, law and international relations*, Cheltenham, Edward Elgar Publishing, 2019, pp. 33-52.

³⁵ Martin Weiler, *op. cit.*, p. 656:

‘The extraterritorial application of human rights treaties such as the ICCPR comes into play when a State interferes with an individual's human rights while the individual is not situated in the territory of that State.²¹ Such a scenario represents the norm when it comes to surveillance. The NSA spying scandal revealed that States do not restrict their spying activities to their territory but also conduct spying operations on foreign soil’.

operations³⁶. The FVYE had showed their opposition³⁷ to Resolution No. A/RES/69/166 of 18 December 2014³⁸ and persisted in their objections, provoking harsh criticism in the subsequent works of the General Assembly³⁹ and the Human Rights Council⁴⁰. Lacking substantive norms, the programmatic nature of these resolutions created the expectation that their principles could be incorporated in a multilateral treaty – e.g., an additional Protocol

³⁶ Specifically, the FVYE alleges that Article 2(1) of the ICCPR should be interpreted as cumulatively requiring that a person is both in the territory and under the jurisdiction of a state in order to challenge the breaching of the human right to privacy. This interpretation hardly fits with what Prof. Pastor Ridruejo defines as a ‘concession to particularism’ – José Antonio Pastor Ridruejo, *op. cit.*, p. 212 – and raises concerns on the prohibition of discrimination set forth, *inter alia*, under Article 4(1) of the ICCPR and on the principles of proportionality (Article 5(2) of the ICCPR). In the end, it affects the state’s own citizens since the virtual “internal/external” dimensions cannot be clearly distinguished – see Kristian P. Humble, “International law, surveillance and the protection of privacy”, *The International Journal of Human Rights*, Vol. 25, No. 1, 2021, pp. 1-25, p. 8 ff., referring to the United Kingdom for example.

³⁷ According to Riccardo Pisillo Mazzeschi, *op. cit.*, pp. 49-63, in the field of human rights the *opinio iuris* that includes, for example, the declarations of states, multilateral treaties, resolutions of international organisations, and other soft law acts, prevails over the one of *diuturnitas* because of the states’ reluctance in conforming to a constant practice in time. According to Niels Petersen, “The Role of Consent and Uncertainty in the Formation of Customary International Law”, in Brian D. Lepard, *Reexamining Customary International Law*, Cambridge, Cambridge University Press, 2017, pp. 111-130, p. 129:

‘[...] persistent objection should not be permitted in cases of a customary norm based on certain compelling ethical principles, such as fundamental human rights. Allowing persistent objection with regard to fundamental rights would permit particular governments to oppose normative developments to the detriment of their population under the pretext of cultural exceptionalism [...] Cultural differences can, instead, be legitimately taken into account by allowing states to exercise a margin of discretion with regard to the solution of conflicts between competing values. Therefore, states have to give reasons to justify their behavior if they want to restrict specific human rights’.

³⁸ Records of the meeting No. 54 of the General Assembly A/C.3/69/SR.54 of 25 November 2014, p. 3:

‘[...] (New Zealand) said that his Government’s domestic legal framework to protect the privacy of individuals included robust oversight mechanisms and was consistent with the relevant human rights obligations. [...] In that regard, his delegation understood article 2.1 of the International Covenant on Civil and Political Rights and the interpretative guidance provided by the Human Rights Committee in paragraph 10 of General Comment No. 31 to be the appropriate legal standard, and interpreted the resolution accordingly. The wish of the delegation of Brazil for the draft resolution to assert extraterritoriality where effective control over communications infrastructure existed, wherever located, would have constituted an unwarranted extension of international law’.

³⁹ Micheal Yilma Kinfe, *loc. cit.*

⁴⁰ Resolution of the Human Rights Council No. A/HRC/27/37 of 30 June 2014, p. 11:

‘The Human Rights Committee has been guided by the principle, as expressed even in its earliest jurisprudence, that a State may not avoid its international human rights obligations by taking action outside its territory that it would be prohibited from taking “at home”. This position is consonant with the views of the International Court of Justice, which has affirmed that the International Covenant on Civil and Political Rights is applicable in respect of acts done by a State “in the exercise of its jurisdiction outside its own territory”, as well as articles 31 and 32 of the Vienna Convention on the Law of Treaties. The notions of “power” and “effective control” are indicators of whether a State is exercising “jurisdiction” or governmental powers, the abuse of which human rights protections are intended to constrain. A State cannot avoid its human rights responsibilities simply by refraining from bringing those powers within the bounds of law. To conclude otherwise would not only undermine the universality and essence of the rights protected by international human rights law, but may also create structural incentives for States to outsource surveillance to each other’.

based on Article 17 of the ICCPR⁴¹. However, the use of consensus⁴² hampered an agreement on the rules to which states would align their behaviour for *diuturnitas*⁴³. As a result, any speculation on the development of a customary, universal rule on the right to privacy must be discarded⁴⁴.

In 2015, the Human Rights Council nominated a Special Rapporteur for the right to privacy⁴⁵ – Prof. Cannataci had his mandate renewed until 2021, when he was replaced by Prof. Brian Nougères⁴⁶ – who is currently in charge of producing periodic reports⁴⁷ and of releasing commentaries on national politics and legislation following the issuance of a request for information from a specific state. Other important initiatives have been launched by the UN General Secretary, the body adopted a Roadmap for Digital Cooperation in July

⁴¹ See the Opinion of the EDPS on *the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows" and on the Communication from the Commission to the European Parliament and the Council on "the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU"*, Brussels, 20.02.2014, p. 16, and the Opinion of the Article 29 DPWP No. 04/2014 on *surveillance of electronic communications for intelligence and national security purposes*, Brussels, 10.04.2014.

⁴² Luis Miguel Hinojosa Martínez, “¿Provocará la regla del consenso la destrucción de la OMC?”, *ICE una política comercial para reconstruir la globalización*, No. 922, 2021, pp. 1-16, and Micheal Yilma Kinfé, *loc. cit.*

⁴³ Jaime Orúa Orúa, 2009, *op. cit.*, p. 218, highlights four elements to upgrade a UN Resolution’ value to the one of customary international law: first, the intention of the parties; second, the majority by which it is approved; third, its content and, fourth, the practice of the states. Riccardo Pisillo Mazzeschi, *op. cit.* p. 49 ff., states that in the human rights field the *opinio iuris* represents the cornerstone for the establishment of customary rules.

⁴⁴ Rebekah Dowd, *The Birth of Digital Human Rights*, London, Palgrave Macmillan, 2022. William A. Schabas, *The Customary International Law of Human Rights*, Oxford, Oxford University Press, 2021, p. 94 ff., recalls that in order not be bound by a customary rule, persistent objectors must consistently oppose to its emergence and must keep objecting after crystallisation has occurred. He also recalls that according to the Report of the International Law Commission No. A/73/10 of 30 April-1 June and 2 July-10 August 2018, Seventieth session, p. 152: ‘the objection of a significant number of States to the emergence of a new rule of customary international law prevents its crystallization altogether (because there is no general practice accepted’.

⁴⁵ Resolution of the UN Human Rights Council No. A/HRC/28/16 of 26 March 2015.

⁴⁶ Available at www.ohchr.org.

⁴⁷ Resolution of the UN Human Rights Council No. A/HRC/37/62 of 25 October 2018, *Report of the Special Rapporteur on the right to privacy*.

2018⁴⁸ with the participation of the Council of the EU⁴⁹, and the Economic and Social Council, which has adopted a handful of resolutions on digital technologies⁵⁰.

The delay in responding to privacy concerns related to new technologies left the UN no choice but to rely on existing legal frameworks and soft law instruments in an eclectic manner⁵¹. Recognising the added value of the first international binding instrument adopted in Europe, some delegations went back to the Council of Europe's⁵² Convention 108⁵³, in which, for example, 'the right to be forgotten' had been successfully recognised by the European Court of Human Rights (ECtHR). Given that the mass-surveillance threat was ongoing⁵⁴, the UN Human Rights Council presented a second report⁵⁵ in session No. 39 of 2018 recalling continental principles, standards, and best practices on the promotion and protection of the right to privacy⁵⁶ with the following words:

⁴⁸ See the UN General Secretary Resolution No. A/74/821 of 29 May 2020, *Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation*. Also, visit the official website of the UN, available at www.un.org.

⁴⁹ Esa Paasivirta and Thomas Ramopoulos, "UN General Assembly, UN Security Council and UN Human Rights Council", in Ramses A. Wessel and Jed Odermatt, *Research Handbook on the European Union and International Organizations*, Cheltenham, Edward Elgar Publishing, 2019, pp. 58-81, explains that each year the Council of the EU adopts a list of priorities for Human Rights Fora based on an underlying multiannual Action Plan on Human Rights and Democracy. The one for 2020-2024 looks for pointing out cases in which new technologies can contribute to enhance human rights – see the official website available at www.ec.europa.eu and the one adopted in 2021 in Council of the EU, *Council Conclusions on EU Priorities in UN Human Rights Fora in 2021*, 6326/21, Brussels, 22 February 2021, p. 9.

⁵⁰ Article 62(2) of Charter of the UN: 'It may make recommendations for the purpose of promoting respect for, and observance of, human rights and fundamental freedoms for all'. See, for example, the Economic and Social Council Resolutions: No. E/RES/2021/10 of 8 June 2021, *Socially just transition towards sustainable development: the role of digital technologies on social development and well-being of all*; No. E/RES/2021/28 of 22 July 2021, *Assessment of the progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society*; No. E/RES/2021/29 of 22 July 2021, *Science, technology and innovation for development*, and No. E/RES/2021/30 of 22 July 2021, *Open-source technologies for sustainable development*.

⁵¹ Micheal Yilma Kinfe, *op. cit.*, p. 497:

[...] not only has the process been gradual and incremental but also considerably eclectic in that the content of the resolutions tend to be significantly influenced by various sources. One sees clear marks of the jurisprudence of judicial and quasi-judicial bodies such as the Human Rights Committee and the European Court of Human Rights (ECtHR), IBRs initiatives as well as a number of thematic reports of the UN Special Rapporteurs'.

⁵² Resolution of the Human Rights Council No. A/HRC/28/39 of 19 December 2014, para. 41.

⁵³ See *infra*.

⁵⁴ In 2016, the Israeli spyware Pegasus was discovered by the Arab human rights defender Ahmed Mansoor. Pegasus was designed to access files, messages, photos and passwords, listens to calls, and retrieve audio recording, camera or geolocation tracking of iOS and Android smartphones. The European Parliament validated the constitution of a commission of inquiry to investigate on EU law breaches perpetrated by some of the Member States, among which Hungary and Poland stand out. See "Le Parlement européen valide la constitution de sa commission d'enquête sur l'utilisation du logiciel espion Pegasus dans l'UE", *Bulletin Quotidien Europe*, No. 12908, 11.3.2022.

⁵⁵ Resolution of the Human Rights Council No. A/HRC/39/29 of 3 August 2018, para. 1.

⁵⁶ The Organisation for Economic Cooperation and Development (OECD) in which the EU has a *de facto* membership status – see Flovi Vlastou-Dimopoulou, "Organisation for Economic Co-operation and Development (OECD)", in Ramses A. Wessel and Jed Odermatt, *op. cit.*, pp. 316-337 – has been promoting an international policy for the protection of personal data with its non-binding OECD, *Guidelines Governing*

‘[...] global consensus on minimum standards that should govern the processing of personal data by States’ existed⁵⁷ thanks not only to the Council of Europe’s framework but to the European Union’s one too since the latter was destined to have ‘global implications’⁵⁸.

Also, ‘domestic legal obligations’ and other relevant ‘commitments’ were considered⁵⁹, which ‘open[ed] the door for, and legitimize[d] the attempt so far, of the discourse to draw from best practices in many jurisdictions particularly the European (data) privacy system’⁶⁰.

1.2. The right to respect for private and family life and the Council of Europe’s Convention

108

Already in the 1950s, the Council of Europe inserted Article 8 on the right to a private and family life⁶¹, which echoed the ideas agreed upon the UDHR⁶². Unlike the latter, Article

the Protection of Privacy and Transborder Flows of Personal Data, Paris, 1980 (Privacy Guidelines). The Privacy Guidelines were elaborated under the influence of the US and looked for a balance between privacy and information needs. However, these Guidelines were unable to bring about sufficient equivalence to guarantee the free movement of data between the OECD states according to Graham Pearce and Nicholas Platten, “Achieving Personal Data Protection in the European Union”, *Journal of Common Market Studies*, No. 36, 1998, pp. 529-548, p. 531. Thus, they were complemented by the OECD, *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* of 2007, and lastly updated in 2013. Other interesting instruments concerning privacy have been adopted and are available at www.oecd.org. The Asia-Pacific Economic Cooperation adopted a soft-law *Privacy Framework*, Singapore, 2004 (updated in 2015), available at www.apec.org, while the Association of Southeast Asian Nations incorporated a *Framework on Personal Data Protection*, Yakarta, 2016, available at www.asean.org.

⁵⁷ The principles recalled were: the principles of fairness, lawfulness and transparency; the fact that the consent must be freely, specifically, informed and unambiguously given; the principles of necessity and proportionality for which personal data must be processed for a legitimate and specified purpose; the period of storage that must be limited, and data must be accurate, anonymised and pseudonymised; the principle of purpose limitation; the principles of security and confidentiality; the principle of accountability, and a high level of protection must be ensured to sensitive data. The resolution maintained that: ‘At a minimum, the persons affected have a right to know that personal data has been retained and processed, to have access to the data stored, to rectify data that is inaccurate or outdated and to delete or rectify data unlawfully or unnecessarily stored’. Also, the establishment of an internal supervisory mechanism was mentioned: ‘[...] requirements related to the design of products and services, such as privacy by design and privacy by default, are essential tools for safeguarding the right to privacy’. Finally, the report referred to independent oversight bodies for safeguarding the human rights.

⁵⁸ Resolution of the Human Rights Council No. A/HRC/39/29 A/HRC/39/29 of 3 August 2018, para. 1. Matteo E. Bonfanti, *op. cit.*, *in fine*, affirms that Article 8 of the ECHR ensures wider protection than Article 17 of the ICCPR which confers Europe and, specifically, the EU, the most progressive role in the data protection field.

⁵⁹ Resolution of the Human Rights Council No. A/HRC/34/7 of 23 March 2017.

⁶⁰ Micheal Yilma Kinfé, *op. cit.*, p. 499.

⁶¹ Article 8 of the ECHR:

- ‘1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others’.

See the commentary of Juan Antonio Carrillo Salcedo, “The European Convention on Human rights”, in Félipe Gómez Isa and Koen de Feyter, *International Human rights Law in a Global Context*, Deusto, HumanitarianNet, 2009, pp. 631-688. On the difference between the right to respect for private life and the right to family life see Riccardo Pisillo Mazzeschi, *op. cit.*, pp 397-404.

⁶² See the Preamble and Article 8(2) of the ECHR.

8 of the ECHR does not refer to privacy itself⁶³ but rather sticks to the French wording *vie privée*, giving rise to contradictory interpretations depending on the reader's cultural background⁶⁴. As with the ICCPR, Article 8 of the ECHR is intended to impose both negative and positive obligations to the contracting parties⁶⁵ – among which, we find all the Member States of the EU⁶⁶ – and, despite its specific reference to ‘public authority’, it has also been recognised *Drittwirkung* effect⁶⁷. ECtHR case-law extended the scope of Article 8 of the ECHR so as to include a ‘constellation of rights’ shaping the right to respect for a

⁶³ Gloria González Fuster, *op. cit.*, p. 82, noted that such a formulation was probably due to the French expression *vie privée*. The author highlights (p. 88 ff.) that the Recommendation of the Parliamentary Assembly of the Council of Europe No. 890 on *the protection of personal data*, Strasbourg, 1 February 1980, advanced the possibility to amend the ECHR to insert a specific right to the protection of personal data, yet ‘[the Committee of ministers and the Steering Committee for Human Rights] suggested that it was preferable to first acquire more experience on the application of Convention 108, while at the same time working towards sector-specific Recommendations complementing it’.

⁶⁴ Matteo E. Bonfanti, *loc. cit.*, clarifies that “private life” should be intended as a specification of the huger concept of “privacy” and, specifically, it refers to the “institutionalised” areas of privacy like: physical and mental integrity; intimacy; identity; sexual behaviour, and personal information or data. Confront *Niemietz v Germany*, No. 13710/88, 16 December 1992, CE:ECHR:1992:1216JUD001371088, § 29:

‘The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of “private life”. However, it would be too restrictive to limit the notion to an “inner circle” in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings’.

⁶⁵ Matteo E. Bonfanti, *op. cit.*, p. 469, and, among others, *Jivan v Romania*, No. 62250/19, 8 February 2022, CE:ECHR:2022:0208JUD006225019, § 31:

‘[...] Article 8 cannot be considered applicable each time an individual’s everyday life is disrupted, but only in the exceptional cases where the State’s failure to adopt measures interferes with that individual’s right to personal development and his or her right to establish and maintain relations with other human beings and the outside world. It is incumbent on the individual concerned to demonstrate the existence of a special link between the situation complained of and the particular needs of his or her private life’.

⁶⁶ Whether and how far the EU is bound by the conventional commitments assumed by its Member States in the human rights field is controversial. “Whether” because the theory on “functional succession”, and the CJEU’s judgments thereto, is not applicable to non-exclusive competences – see, for example: Noëlle Quénivet, “Binding the United Nations to Customary (Human Rights) Law”, *International Organizations Law Review*, No. 379, 2020, pp. 379-417; Robert Schütze, *The ‘succession doctrine’ and the European Union*, Cambridge, Cambridge University Press, 2014, pp. 91-119; Jan Wouters, Jed Odermatt, and Thomas Ramopoulos, “Worlds Apart Comparing the Approaches of the European Court of Justice and the EU Legislature to International Law”, in Marise Cremona and Anne Thies, *The European Court of Justice and External Relations Law*, United Kingdom, Hart Publishing, 2014, pp. 249-280, and Mathias Forteau, “Le droit applicable en matière de droits de l’homme aux administrations territoriales gérées par des organisations internationales”, in Ronny Abraham, *Le droit international des droits de l’homme applicable aux activités des organisations internationales*, Paris, A. Pedone, 2009, pp. 7-34, p. 24 ff. “How” because the founding Treaties do not impose straightforward to the EU an obligation to protect and fulfill human rights, but to ‘uphold and promote’ its values and interests, ‘contribute’ to the protection of human rights, be ‘guided by and advance’ in the wider world, *inter alia*, the universality and indivisibility of human rights and fundamental freedoms, and ‘consolidate and support’ human rights – see Article 3(5), 21(1), and 21(3) TEU and Lorand Bartels, “The EU’s Human Rights Obligations in Relation to Policies with Extraterritorial Effects”, *European Journal of International Law*, Vol. 25, No. 4, 2014, pp. 1071-1092. In the specific case of the ECHR, the CJEU in C-601/15 PPU, *J. N. v Staatssecretaris voor Veiligheid en Justitie*, 15 February 2016, EU:C:2016:84, para. 45, clarified that until the EU will not accede to it, the ECHR is not an instrument formally integrated within the EU but its dispositions enter in the EU legal order as general principles of law – see also *infra*.

⁶⁷ *Jivan v Romania*, § 40: ‘These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves’.

private and a family life into a ‘prism with multiple facets’⁶⁸. Among other readings, by the end of the 60s, Article 8 ECHR was revisited in light of the rise of advancing technology⁶⁹.

This interpretation paved the way toward the adoption of a first international instrument of a binding nature on the protection of personal data – namely, Convention 108⁷⁰. The situation within the Council of Europe at the end of the ‘70s was that seven of the organisation’s states had adopted national laws on the protection of personal data – namely Austria, Denmark, France, Germany, Luxembourg, Norway, and Sweden –, but only three states had incorporated these into their constitutions – Portugal, Spain⁷¹, and Austria⁷². Other members neither recognised the right to protection of personal data in their constitutions⁷³, nor were they equipped with a *corpus iuris* on the matter. Indeed, discussions within national parliaments were still ongoing when the Council of Europe’s Convention 108 was agreed and its text became the point of reference to fill in internal legislative *lacunae*⁷⁴. Today, all the states of the Council of Europe, including the Member States of the EU, have ratified Convention 108⁷⁵ and another eight non-members have joined it, namely: Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia, and Uruguay. Being open to signing

⁶⁸ Giulia Tiberi, “Riservatezza e protezione dei dati personali”, in Marta Cartabia, *Il diritto in azione: universalità e pluralismo dei diritti fondamentali nelle Corti europee*, Bologna, Mulino, pp. 349-387, p. 362.

⁶⁹ Recommendations of the Parliamentary Assembly of the Council of Europe No. 509 on *Human rights and modern scientific and technological developments*, Strasbourg, 31 January 1968; Resolution of the Committee of Ministers No. 73(22) on *the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*, Strasbourg, 26 September 1973, and Resolution of the Committee of Ministers No. 74(29) on *the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*, Strasbourg, 20 September 1974. Also, see Andrea Blasi, “La protezione dei dati personali nella Giurisprudenza della Corte europea dei diritti dell’uomo”, *Rivista internazionale dei diritti dell’uomo*, Vol. 12, No. 2, 1999, pp. 543-559.

⁷⁰ Today, it counts with fifty-five adhesions among which eight states that are not part of the Council of Europe – information available at www.coe.int.

⁷¹ Specifically, the Constitución Española, *Boletín Oficial del Estado* No. 311, 29.12.1978, sets forth in its Article 18(4) that the legislator should establish the limits to use of information technology in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights. An overview of the Member States’ constitutions after the entry into force of the Lisbon Treaty is given by María Rosa Ripollés Serrano, *Constituciones de los 27 Estados miembros de la Unión Europea*, Madrid, Congreso de los Diputados, 2010, and English versions are available at www.constituteproject.org.

⁷² See the Explanatory Report of the Council of Europe on *the Convention for the protection of individuals with regard to Automatic Processing of Personal Data*, Strasbourg, 21 January 1981, p. 2.

⁷³ H. Franken and A. K. Koekoek, “The protection of fundamental rights in a digital age”, in VV. AA., *Convergence of legal systems in the 21st century: general reports delivered at the XVth internet*, Brussels, Bruylant, 2002, pp. 1147-1164, instead, focus on Canada, Japan, Denmark, and The Netherlands to highlight their inadequacy to new challenges arising from digitality.

⁷⁴ The United Kingdom’s Data Protection Act was adopted in 1984 after the Council of Europe’s Convention 108 entered into force. In 1998 the Data Protection Act was amended to be interpreted in the light of Article 8 ECHR thanks to the adoption of the Human Rights Act 1998 and it was subsequently derogated by the Data Protection Act of 2018. The information is available at www.legislation.gov.uk.

⁷⁵ Consult the official website at www.coe.int.

by non-member countries⁷⁶, Convention 108 represented a first attempt to spread continental standards of protection worldwide⁷⁷.

Convention 108 lays down a minimum core of principles⁷⁸ for the processing of ‘personal data’, that is, ‘any information relating to an identified or identifiable individual’⁷⁹, in the frame of automated personal data files and automatic processing of personal data in the public and private sectors⁸⁰. Contracting parties are free to adopt more rigorous standards in their domestic law⁸¹. These principles state that the automatic processing of personal data be of ‘quality’⁸², which means that personal data must be:

- obtained and processed fairly and lawfully;
- stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are stored;
- accurate and, where necessary, kept up to date, and

⁷⁶ Article 23(1) of the Convention 108 sets forth: ‘After the entry into force of this Convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this Convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee’. The procedure is explained in the document on the Council of Europe, *Accession by States which are not member States of the Council of Europe*, Strasbourg, 2019, available at www.rm.coe.int. Third countries invited to take part of it in the following years are listed in the document of the Council of Europe, *Non-members States of the Council of Europe: Five years validity of an invitation to sign and ratify or to accede to the Council of Europe’s treaties*, Strasbourg, 16 February 2022, available at the same webpage. The European Community was invited to take part in Convention 108 in 1999 through an Amending Protocol according to Article 4(2) of the *Amendments approved by the Committee of Ministers*, Strasbourg, 15 June 1999, available at www.rm.coe.int: ‘The European Communities may accede to the Convention’. However, not all the parties to the Convention 108 notified their acceptance of the proposed amendments as required by its Article 21(6) – e.g., see the note No 44 in the chart of signatures and ratifications of Treaty 108 available at www.coe.int, and the Romanian declaration in Council of the EU, *Recommendation for a Council Decision authorising the opening of negotiations on the modernisation of Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (EST 108) and the conditions and modalities of accession of the European Union to the modernised Convention*, 6176/13 DCL 1, Brussels, 30 January 2019, p. 18. Therefore, the amendments have never entered into force and the European Community has never taken part to Convention 108.

⁷⁷ Article 23 of Convention 108 requires the unanimous vote of the contracting states entitled to set in the Committee of Ministers.

⁷⁸ Article 4 of Convention 108.

⁷⁹ Article 2(a) of Convention 108.

⁸⁰ Article 3(b) and (c) of Convention 108. The latter specifies that “automated processing” includes ‘the storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination’. Article 3(2)(c) allowed states parties to declare their willingness to extend the scope of Convention 108 to ‘personal data files which are not processed automatically’.

⁸¹ Article 11 of Convention 108: ‘None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this Convention’.

⁸² Article 5 of Convention 108.

- preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which the data is stored.

In practice, the interpretation of the Convention 108 has been built upon Article 8 of the ECHR⁸³. In *Leander v Sweden*, the ECtHR ruled that the retention⁸⁴ and release of data related to the private life of an individual, together with the impossibility for him/her to refute it, constitutes an interference of Article 8(1) ECHR⁸⁵ and that enhanced safeguards are needed in case personal data is processed in an automated manner⁸⁶. Interferences with Article 8(1) ECHR are not mitigated by the fact that data is encrypted⁸⁷ as these security features⁸⁸ do not apply to “related data” or metadata including the identities and geographic location of the sender and recipient of a message, as well as the equipment through which communication is transmitted⁸⁹. However, the ECtHR has ambiguously admitted that

⁸³ *S. and Marper v the United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008, CE:ECHR:2008:1204JUD003056204, § 103: ‘The protection of personal data is of fundamental importance to a person’s enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention’. Further jurisprudence is analysed by Özgür Heval Çımar, “The current case law of the European Court of Human Rights on privacy: challenges in the digital age”, *International journal of human rights*, Vol. 25, No. 1, 2021, pp. 26-51.

⁸⁴ See *Amann v Switzerland*, No. 27798/95, 16 February 2000, CE:ECHR:2000:0216JUD002779895, concerning the recording of a telephone call on ‘activities of a professional or business nature’ between a depilator seller in Switzerland and a woman from the Soviet embassy, § 45 and § 65. Similarly is the case *Halford v United Kingdom*, No. 20605/92, 25 June 1997, CE:ECHR:1997:0625JUD002060592, § 42, where the intercepted information was alleged to be discriminatory used in the labor domain. In *S. and Marper v the United Kingdom*, § 73, the ECtHR found that ‘[g]iven the nature and the amount of personal information contained in cellular samples, their retention per se must be regarded as interfering with the right to respect for the private lives of the individuals concerned’.

⁸⁵ *Leander v Sweden*, No. 9248/81, 26 March 1987, CE:ECHR:1987:0326JUD000924881, § 48, concerning a Swedish national who was fired following a control made by the national police board which revealed that a secret police-register stored information concerning him. In case of data collected in public areas, the ECtHR seems to raise the threshold to ‘systematic collection and storage’ of data – i.e. in *Rotaru v Romania* [GC], No. 28341/95, 4 May 2000, CE:ECHR:2000:0504JUD002834195, § 44, where studies, political activities and criminal record were filed and held by police authorities – or to ‘systematic and permanent record’ – i.e., *P.G. and J.H. v the United Kingdom*, No. 44787/98, 25 December 2001, CE:ECHR:2001:0925JUD004478798, § 57, with respect to the recording of voices of individuals while being charged at the police station and held in their cells. However, the former case raised perplexities as to whether the information fell within the protection granted by Article 8(1) of the ECHR since this was made public – see the partly dissenting opinion of judge Bonello.

⁸⁶ *S. and Marper v the United Kingdom*, § 103.

⁸⁷ *Amann v Switzerland*, § 69, and *S. and Marper v the United Kingdom*, § 67.

⁸⁸ Article 7 of Convention 108: ‘Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination’. The ECtHR also affirmed that an interference existed as soon as personal data were stored in the Confederation’s card index, notwithstanding their sensitive nature (§ 70).

⁸⁹ *Big Brother Watch and Others v the United Kingdom* [GC], Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021, CE:ECHR:2021:0525JUD005817013, § 342:

‘[...] any intrusion occasioned by the acquisition of related communications data will be magnified when they are obtained in bulk, since they are now capable of being analysed and interrogated so as to paint an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with’.

although ‘the interception, retention and searching of related communications data’ must take place with the same safeguards as content data, the underlying regulations ‘may not necessarily have to be identical in every respect to those governing the treatment of content’⁹⁰.

In addition, Convention 108 pays attention to ‘special categories of personal data’, such as criminal convictions⁹¹. In *Friedl v Austria*⁹², the European Commission of Human Rights⁹³ found that the taking (and subsequent retention) of photographs of an individual suspected of planning a criminal activity when meeting with several persons in a public space did not amount to an interference with Article 8(1) ECHR⁹⁴, but the establishment of the individual’s identity and the recording of personal data ‘closely related to his private affairs’ did⁹⁵. In its judgment, the European Commission of Human Rights considered that the keeping of records related to criminal offences should be considered as necessary in a democratic society for the prevention of crimes ‘and that even if no criminal proceedings are subsequently brought and there is no reasonable suspicion against the individual concerned in relation to any specific offence, special considerations, such as combating organised terrorism, can justify the retention of the material concerned’⁹⁶. However, in its historical judgment *S. and Marper v the United Kingdom*, the ECtHR ruled that similarly to photographs and voice recordings, the retention of fingerprints related to an identified or identifiable individual constitutes *per se* interference with Article 8(1) ECHR, ‘notwithstanding their objective and irrefutable character’⁹⁷. The ECtHR found that the retention of cellular samples that ‘contain much sensitive information about an individual’⁹⁸ and of DNA profiles that are apt to discern an individual’s ethnic origin – which ‘makes their retention all the more sensitive and susceptible of affecting the right to private life’⁹⁹ – have

The ECtHR then found (§ 423) that the different regime applicable to “related communications” by the United Kingdom was justifiable and lawful before Article 8 of the ECHR. However, the provision of different retention periods was lacking a legal basis “foreseeable” by the individual.

⁹⁰ *Big Brother Watch and Others v the United Kingdom*, § 364.

⁹¹ Article 6 of Convention 108: ‘Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions’.

⁹² *Friedl v Austria*, No. 15225/89, 19 May 1994, CE:ECHR:1994:0519REP001522589.

⁹³ Abolished by Protocol No 11 to the Convention for the Protection of Human Rights and Fundamental Freedoms, Restructuring the Control Machinery Established therein, ETS 155, signed in Strasbourg on 11 May 1994, entered into force on 11 November 1998.

⁹⁴ *Friedl v Austria*, § 51.

⁹⁵ *Ibid.*, § 52.

⁹⁶ *Ibid.*, § 66.

⁹⁷ *S. and Marper v the United Kingdom*, § 85.

⁹⁸ *Ibid.*, § 96.

⁹⁹ *Ibid.*, § 76.

more impact on the right to a private life than fingerprints. Despite this, the ECtHR firmly maintained that:

‘[...] the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants’ right to respect for private life and cannot be regarded as necessary in a democratic society’¹⁰⁰.

Article 8 of Convention 108 sets forth guarantees applicable to any processing activity that seeks to: establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file; obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to the individual are stored in an automated data file, as well as the communication to the individual of such data in an intelligible form¹⁰¹; obtain, where applicable, the rectification or erasure of such data if it has been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of the Convention¹⁰²; contain a mechanism for recourse if a request for confirmation or communication, rectification or erasure is not complied with.

Exceptions to the above-mentioned principles are accounted for in respect to: the principle of legality; the principle of the necessity in a democratic society to protect the state’s security, public safety, the monetary interests of the state or the suppression of

¹⁰⁰ *Ibid.*, § 125.

¹⁰¹ *Gaskin v the United Kingdom* [GC], No. 10454/83, 7 July 1989, CE:ECHR:1989:0707JUD001045483, § 37, where the ECtHR affirmed that the refusal of the request to access an own child care records constitutes an interference with Article 8(1) of the ECHR. Specifically, the data subject’s request should be balanced with the requisite of confidentiality of the contributor – i.e., medical practitioners, school teachers, police and probation officers, social workers, health visitors, foster parents and residential school staff – when either is not available or improperly refuses consent (§ 49).

¹⁰² *Khelili v Switzerland*, No. 16188/07, 8 March 2012, CE:ECHR:2011:1018JUD001618807, agreeing that Article 8(1) ECHR had been breached for not having erased the applicant’s name from the police register where she was erroneously labelled as prostitute.

criminal offences¹⁰³, and the data subject or the rights and freedoms of others¹⁰⁴. Sanctions and remedies for any infringement of Convention 108 must be set down by the own Member States¹⁰⁵. Specifically, Article 8(2) ECHR sets forth that any exception must be:

‘[...] in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others’¹⁰⁶.

On this basis, the ECtHR has developed a model case-law on (bulk) communication interceptions¹⁰⁷ the lawfulness of which is assessed on the basis of six minimum safeguards: the nature of the offences; the definition of the categories of people liable to have their communications intercepted; the limit on the duration of the interception; the procedure to be followed for examining, using and storing the obtained data; the precautions to be taken when communicating the data to other parties, and the circumstances in which intercepted

¹⁰³ Article 9(2) of Convention 108. See the Committee of Ministers Recommendation R (87) 15 regulating *the use of personal data in the police sector*, Strasbourg, 17 September 1987, and the following related reports: Report on the *first evaluation of Recommendation R (87) 15 regulating the use of personal data in the police sector*, Strasbourg, 1994; Report on the *second evaluation of Recommendation R (87) 15 regulating the use of personal data in the police sector*, Strasbourg, 1998, and Report on the *third evaluation of Recommendation R (87) 15 regulating the use of personal data in the police sector*, Strasbourg, 2002. See also Joseph Aka Cannataci and Mireille Martine Caruana, “Report: Recommendation R (87) 15 – Twenty-five years down the line”, *Statewatch*, 10 October 2013, available at www.statewatch.org. Analyses on the ECtHR jurisprudence on the protection of personal data for law enforcement purposes is made by: Kirill Belogubets, “The protection of personal data in the context of law enforcement: recent case law of the European Court of Human Rights”, *ERA Forum*, Vol. 22, 2021, pp. 231-243; Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, Berlin/Heidelberg, Springer-Verlag, 2012, pp. 96-102, and Gianfranco Marullo, “Il ruolo e le attività dei servizi di intelligence e delle forze di polizia nella lotta alla criminalità ed al terrorismo nei paesi dell’Unione Europea, nel rispetto della Convenzione del Consiglio d’Europa sui diritti dell’uomo”, in M. Cherif Bassiouni, *La Cooperazione internazionale per la prevenzione e la repressione della criminalità organizzata e del terrorismo*, Milano, Giuffrè, 2005, pp. 187-208.

¹⁰⁴ Article 9(2) of Convention 108.

¹⁰⁵ Article 11 of Convention 108.

¹⁰⁶ *Roman Zakharov v Russia*, No. 47143/06, 4 December 2015, CE:ECHR:2015:1204JUD004714306, § 227. See, *inter alia*, *Kennedy v the United Kingdom*, No. 26839/05, 18 August 2010, CE:ECHR:2010:0518JUD002683905, § 130.

¹⁰⁷ In *Kennedy v the United Kingdom*, § 118 ff.; *Liberty and Others v the United Kingdom*, No. 58243/00, 1 October 2008, CE:ECHR:2008:0701JUD005824300, §56; *Weber and Saravia v Germany*, No. 54934/00, 26 June 2006, CE:ECHR:2006:0629DEC005493400, §7, and *Klass and Others v Germany*, No. 5029/71, 6 September 1978, CE:ECHR:1978:0906JUD000502971, §34, the ECtHR maintained that the provision of secret monitoring systems is a “threat” of surveillance and, consequently, its mere existence represents an interference with Article 8(1) ECHR. However, in *Roman Zakharov v Russia*, §170, the ECtHR specified that such a compliant should follow this analysis: first, the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it; second, the availability and effectiveness of remedies at the national level. According to it:

‘There is therefore a greater need for scrutiny by the Court, and an exception to the rule denying individuals the right to challenge a law *in abstracto* is justified. In such cases the individual does not need to demonstrate the existence of any risk that secret surveillance measures were applied to him. By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures’.

data may or must be erased or destroyed¹⁰⁸. In its jurisprudence, the ECtHR cumulatively evaluates the principle of legality – in terms of foreseeability¹⁰⁹, accessibility and precision¹¹⁰ – and the principle of proportionality or ‘necessity in a democratic society’¹¹¹ for which purpose the former must settle ‘adequate and effective safeguards and guarantees against abuse’¹¹².

In the long-awaited case *Big Brother Watch and Others v the United Kingdom*, the Grand Chamber of the ECtHR identified ‘new threats in the digital domain’¹¹³ which required the creation of new assessment criteria to address the intrusiveness of ‘international communication’ bulk interception systems. Interestingly, the ECtHR pointed out four main stages through which bulk interceptions take place and affirmed that as long as these interceptions continue to take place and evolve, the more intrusive they will become¹¹⁴. The ECtHR highlighted the fact that interception is used to support not only police targeted investigations¹¹⁵, but also the untargeted (or bulk) collection of intelligence material to shield

¹⁰⁸ For example, in *Roman Zakharov v Russia*, § 231.

¹⁰⁹ *Weber and Saravia v Germany*, § 93: ‘It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated [...]. The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures’.

¹¹⁰ *Malone v the United Kingdom*, No. 8691/79, 2 August 1984, CE:ECHR:1984:0802JUD00086917, § 68: ‘[...] the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference’, which was not the case of England and Wales laws. In *S. and Marper v the United Kingdom*, § 99, the ECtHR sentenced that law must set forth: ‘[...] duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness’.

¹¹¹ The ECtHR admits that states retain a margin of appreciation in this assessment: *Roman Zakharov v Russia*, § 232; *Klass and Others v Germany*, § 49, 50 and 59; *Weber and Saravia v Germany*, § 106, and *Kennedy v the United Kingdom*, §§ 153 and 154.

¹¹² *Roman Zakharov v Russia*, § 236. See also *Kennedy v the United Kingdom*, § 155. In *Big Brother Watch and Others v the United Kingdom*, § 361, the ECtHR resumed the following elements: the grounds on which bulk interception is authorised and the circumstances in which an individual’s communications is intercepted; the procedure to be followed for granting authorisation and for selecting, examining and using intercept material; the precautions to be taken when communicating the material to other parties; the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed; procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance; the procedures for independent *ex post facto* review of such compliance, and the powers vested in the competent body in addressing instances of non-compliance.

¹¹³ *Big Brother Watch and Others v the United Kingdom*, § 323: first, communication and related data (or metadata) are intercepted and retained; second, specific selectors – i.e., technical combinations of numbers or letters –, are applied to the retained communications/related communications data; third, the selected communications/related communications data is examined by analysts; and, fourth, data is retained and eventually shared with third parties.

¹¹⁴ *Ibid.*, § 325.

¹¹⁵ *Malone v the United Kingdom*, followed the challenge submitted by Mr. James Malone against the interception, monitoring and recording of conversations on his telephone pursuant to a warrant of the Secretary of State. The ECtHR sentenced (§ 64) that the practice of “tapping” correspondence “[a]s telephone

against foreign threats¹¹⁶. Therefore, circumscribing their scope with regard to the nature of the offences and the categories of people affected is not feasible in the case of bulk interception systems. Four out of six minimum safeguards remain relevant to the creation of new “end-to-end safeguards”¹¹⁷. These are:

- a domestic assessment undertaken by a supervisory body at each stage of the process regarding the necessity and proportionality of the measures, in order to achieve this, each stage of the process must be recorded¹¹⁸;
- a prior independent (not necessarily judicial) authorisation for bulk interception setting down ‘the types or categories of selectors to be used’¹¹⁹;
- a definition of the object and scope of the operation, and
- an *ex post facto* review performed by an independent supervisory authority¹²⁰ (including a non-judicial one¹²¹), without the need to notify the subject of the data interception¹²².

conversations are covered by the notions of “private life” and “correspondence” within the meaning of Article 8 [...] the admitted measure of interception involved an “interference by a public authority” with the exercise of a right guaranteed to the applicant under paragraph 1 of Article 8 [...].

¹¹⁶ *Big Brother Watch and Others v the United Kingdom*, § 345, § 374, and § 375; previously, *Liberty and Others v the United Kingdom*, § 63. In the case of the United Kingdom, section 8(4) of the Regulation of Investigatory Powers Act 2000 regulates bulk interception applied to the so-called ‘external communications’ that are those sent or received outside the British Islands. According to the ECtHR:

‘Whether or not a communication was “external” therefore depended on the geographic location of the sender and recipient and not on the route the communication took to its destination. The distinction between internal and external communications did not, therefore, prevent the interception of internal communications travelling across the United Kingdom’s borders [...] In addition, the definition of “external” was itself sufficiently broad to include cloud storage and the browsing and social media activities of a person in the United Kingdom [...]’.

¹¹⁷ The same rationale was followed by the ECtHR in *Centrum för rättvisa v Sweden* [GC], No. 35252/08, 25 May 2021, CE:ECHR:2021:0525JUD003525208, § 262 ff., that was issued on the same day as the *Big Brother Watch v the United Kingdom*. In this judgment, the ECtHR stated that the Swedish regime lacked sufficient guarantees on three major points: first, the lack of clear rule on destroying intercepted material which does not contain personal data; second, the non-provision of an assessment on the necessity and proportionality of sharing intelligence data to foreign parties as well as the lack of empowerment of the National Defence Radio Establishment to take redress action in case a serious breach to the privacy of individuals occurs and, third, the non-independency of the Inspectorate conducting the *ex post facto* review provided that it had to assess its own activity in supervising bulk interception by National Defence Radio Establishment.

¹¹⁸ *Big Brother Watch and Others v the United Kingdom*, § 356.

¹¹⁹ *Ibid.*, § 354, which was found to be missing in the United Kingdom’s case (§ 383).

¹²⁰ *Ibid.*, § 350.

¹²¹ The ECtHR recognises that although judicial control is preferable, another body respecting the requisites of independence, impartiality and a proper procedure is sufficient to ensure *ex post* oversight on secret surveillance measures – see *Roman Zakharov v Russia*, § 233; *Klass and Others v Germany*, § 55 and § 56, and *Big Brother Watch and Others v the United Kingdom*, § 336. In these terms, the ECtHR found that the Investigatory Powers Tribunal of the United Kingdom ‘[...] provided a robust judicial remedy to anyone who suspected that his or her communications had been intercepted by the intelligence services’ (§ 415).

¹²² *Big Brother Watch and Others v the United Kingdom*, §§ 357-359: ‘The decisions of such authority shall be reasoned and legally binding with regard, *inter alia*, to the cessation of unlawful interception and the destruction of unlawfully obtained and/or stored intercept material’. However, in *Weber and Saravia v Germany*, § 135, the ECtHR maintained that: ‘As soon as notification can be carried out without jeopardising

Notably, the empowerment of national supervisory authorities¹²³ was not foreseen at the time of writing Convention 108, but was added through the First Additional Protocol for the Protection of Individuals with regard to Automatic Processing of Personal Data to the Supervisory Authorities and cross-border data flows on 8 November 2001¹²⁴. With it, national supervisory authorities were called on to ensure states' compliance with their domestic law¹²⁵, the authorities were to operate in full independence¹²⁶. The importance of these laws was confirmed¹²⁷ in *Big Brother Watch and Others v the United Kingdom* where the ECtHR found that bulk interceptions according to section 8(4) of the Regulation of Investigatory Powers Act 2000 were unlawfully authorised by the Secretary of State of the United Kingdom instead of an independent body¹²⁸.

Moreover, the First Additional Protocol to Convention 108 resolved the lack of provision of a regime on transborder data flows¹²⁹ toward non-contracting parties¹³⁰ based on the

the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned'.

¹²³ Article 13 of Convention 108 required the contracting parties to establish one or more authorities – also designated authorities according to Article 15 – to cooperate for the implementation of the treaty and, specifically, to exchange information on each other administrative practice or relating to specific automatic processing carried out in its territory. Only in specific predetermined cases a designated authority could have refused to give its assistance according to Article 16 of Convention 108.

¹²⁴ First Additional Protocol for the Protection of Individuals with regard to Automatic Processing of Personal Data to the Supervisory Authorities and cross-border data flows, ETS No. 181, signed in Strasbourg on 8 November 2001, entered into force on 1 July 2004 – ratified by forty-four parties but not by Belgium, Greece, Iceland, Italy, Malta, Slovenia, and United Kingdom. See also the Report of the European Commission for Democracy through Law (“the Venice Commission”) on *the Democratic Oversight of Signals Intelligence Agencies*, Strasbourg, 20-21 March 2015.

¹²⁵ Article 1 provided for investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities and to hear claims lodged by any person concerning the protection of his/her rights.

¹²⁶ Article 1(2)(b) of the First Additional Protocol to Convention 108.

¹²⁷ *Rotaru v Romania*, § 59:

‘Supervision procedures must follow the values of a democratic society as faithfully as possible, in particular the rule of law, which is expressly referred to in the Preamble to the Convention. The rule of law implies, inter alia, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure [...]’.

¹²⁸ *Big Brother Watch and Others v the United Kingdom*, §377.

¹²⁹ The First Additional Protocol to Convention 108 inserted a new Article 2 to regulate the transborder flow of personal data to a recipient which is not subject to the jurisdiction of a party to the Convention. According to this norm:

‘1. Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer. 2. By way of derogation from paragraph 1 of Article 2 of this Protocol, each Party may allow for the transfer of personal data: a. if domestic law provides for it because of: – specific interests of the data subject, or – legitimate prevailing interests, especially important public interests, or b. if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law’.

¹³⁰ Article 12 of Convention 108 only referred to the transfer of data among contracting parties and maintained that this could be hampered for data protection principles only: a insofar as its legislation includes specific

‘adequate level of protection’ parameter¹³¹. In its previous jurisprudence¹³², the ECtHR clarified that the transmission of data, as well as its use by other authorities, amount to separate interferences with Article 8(1) of the ECHR. Again, the latest judgment on the United Kingdom is pioneering in creating standards for the transfer of data that is stored following bulk interceptions¹³³. The ECtHR found that:

- the circumstances in which such a transfer may take place must be clearly set out in domestic law;
- the transferring state must ensure that the receiving state has in place safeguards capable of preventing abuse and disproportionate interference when handling the data;
- heightened safeguards are necessary when it is clear that material requiring heightened levels of confidentiality – such as confidential journalistic material – is being transferred, and
- the transfer of material to foreign intelligence partners should be subject to independent control.

In the case in question, the ECtHR noted that the material intercepted by the United Kingdom could have been accessed by the FVYE partners according to the British legislation¹³⁴ whose ‘precautions to be taken when communicating intercept material to other parties were sufficiently clear and afforded sufficiently robust guarantees against abuse’¹³⁵. Notably, as far as the receiving party’s safeguards are concerned, the ECtHR established that

regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other party provide an equivalent protection, or when the transfer is made from its territory to the territory of a non-contracting state through the intermediary of the territory of another party, in order to avoid such transfers resulting in circumvention of the legislation of the party referred to at the beginning of this paragraph.

¹³¹ Article 2(1) of the First Additional Protocol to Convention 108. Derogations are allowed only if: specific interests of the data subject, or legitimate prevailing interests, especially important public interests provided by the domestic, or safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law.

¹³² *Weber and Saravia v Germany*, § 79, the case-law quoted therein, and § 123 ff.:

‘The Court finds that the transmission of personal data obtained by general surveillance measures without any specific prior suspicion in order to allow the institution of criminal proceedings against those being monitored constitutes a fairly serious interference with the right of these persons to secrecy of telecommunications. [However,] the Court takes the view that the interference with the secrecy of the communications made by persons subject to monitoring [...] was counterbalanced both by a reasonable limitation of the offences for which data transmission was permitted and by the provision of supervisory mechanisms against abuse’.

¹³³ *Big Brother Watch and Others v the United Kingdom*, § 362.

¹³⁴ *Ibid.*, § 396.

¹³⁵ *Ibid.*, § 399.

that state must guarantee the ‘secure storage of the material and restrict its onward disclosure’¹³⁶, but:

‘This does not necessarily mean that the receiving State must have comparable protection to that of the transferring State; nor does it necessarily require that an assurance is given prior to every transfer’¹³⁷.

As we will further discover in this paper, the ECtHR’s interpretation on adequacy falls short with regard to the assessment conducted by the CJEU in its case-law on mass surveillance regimes, which considers the EU *acquis* on the protection of personal data. Besides, this ruling is inconsistent with the forthcoming regime on transborder flows of personal data. The Second Additional Protocol revising the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 10 October 2018¹³⁸ (Convention 108+), modernised Convention 108 in the light of the latest technological developments while ensuring consistency with EU law¹³⁹. Notably, Convention 108+ expressly refers¹⁴⁰ to the right to the protection of personal data¹⁴¹ while including the following EU principles:

- the extension of the concepts of ‘data processing’, of controller¹⁴² and of sensitive data¹⁴³ while incorporating the concept of ‘data processor’¹⁴⁴;
- the principle of the informed and transparent consent of the data subject¹⁴⁵;
- the right not to be subject to decisions based solely on an automated processing of data¹⁴⁶;
- data protection controllers’ and processors’ liabilities¹⁴⁷, including the implementation of data protection by design and by default principles;

¹³⁶ *Ibid.*, § 395.

¹³⁷ *Ibidem*.

¹³⁸ Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 223, signed in Strasbourg on 10 October 2018 – it counts on eleven ratification among which of one country not part of the Council of Europe.

¹³⁹ Committee on Legal Affairs and Human Rights, *Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (ETS No. 108), and its explanatory report*, Strasbourg, 15 November 2017, para. 10, available at www.pace.coe.int. See, for example, Graham Greenleaf, “A World Data Privacy Treaty: "Globalisation" and "Modernisation" of Council of Europe Convention 108”, in Normann Witzleb, David Lindsay, Moira Paterson, and Sharon Rodrick, *Emerging challenges in privacy law: comparative perspective*, Cambridge, Cambridge University Press, 2014, pp. 92-138.

¹⁴⁰ Council of Europe, *Convention 108+: Convention for the protection of individuals with regard to the processing of personal data*, Strasbourg, 2018, available at www.rm.coe.int.

¹⁴¹ Article 1(3) of Convention 108+.

¹⁴² Article 3(1)-(3) of Convention 108+.

¹⁴³ Article 8 of Convention 108+.

¹⁴⁴ Article 3(4)(f) of Convention 108+.

¹⁴⁵ Articles 7(2) and 8 of Convention 108+.

¹⁴⁶ Article 11(2) of Convention 108+.

¹⁴⁷ Article 12 of Convention 108+.

- the introduction of different – e.g., essential objectives of general public interest – or further – e.g., the impartiality and independence of the judiciary or the prevention – derogation clauses to the principles and rights set forth by Convention 108+¹⁴⁸;
- detailed rules on the transfer of personal data, including the clear specification of the appropriate level of protection¹⁴⁹, and
- enhanced powers, including cooperative powers, for national supervisory authorities¹⁵⁰.

In the case of the transfer of personal data to recipient subject to the jurisdiction of a non-contracting state or an international organisation, Convention 108+ establishes that the transfer must be covered by law or by *ad hoc* or approved and standardised safeguards that are ‘legally binding and enforceable, as well as duly implemented’¹⁵¹. Specifically, any legislative measure authorising such a transfer must concretise: the type of data; the purposes and duration of processing for which the data was transferred; the respect of the rule of law by the country of final destination; the general and sectoral laws applicable within the state or organisation in question, and the professional and security rules which apply there¹⁵². The ‘appropriateness’ of the level of protection conferred by the third party should be evaluated on the basis of the right to effective ‘administrative and judicial’ remedies and the enforceability of the data subject’s rights¹⁵³. Derogations are allowed, according to the principle of proportionality, where: the data subject has given his/her consent or specific interest, and/or where there are prevailing legitimate interests provided by law, and/or the transfer constitutes a necessary and proportionate measure in a democratic society in line with freedom of expression¹⁵⁴. The new rules on transborder flows of data reproduce some of the guarantees the EU had already adopted in the ‘90s, which anticipated the leading role played by the EU in the data protection field.

¹⁴⁸ Article 14 of Convention 108+.

¹⁴⁹ Article 17 of Convention 108+.

¹⁵⁰ Articles 19 and 21 of Convention 108+.

¹⁵¹ Article 17(2) of Convention 108+.

¹⁵² Council of Europe, *Convention 108+ Convention for the protection of individuals with regard to the processing of personal data*, Strasbourg, 2018, available at www.rm.coe.int, p. 28.

¹⁵³ *Ibidem*.

¹⁵⁴ *Ibidem*.

2. The human right to privacy: Paving the way toward the establishment of a European Union's competence on the protection of personal data

The EU's institutional concern for regulating the exchange and protection of personal data gathered strength in the '70s and was in response to the increasing use of information by European and foreign trading companies which urgently demanded coordination in strategic matters¹⁵⁵. As advanced above, domestic debates on the protection of personal data had already started in some European countries under the US or the Council of Europe's influences: the German federal state of Hesse adopted a Data Protection Act in 1970¹⁵⁶, and France adopted its *Loi relative à l'informatique, aux fichiers et aux libertés* in 1978¹⁵⁷.

Legislative works within the European Community were aligned to those of the Council of Europe's under the aegis of an all-inclusive multilateralism where various types of players will be involved. Specifically, the European Community relied upon the work-in-progress Convention 108¹⁵⁸ to promote alignment and convergence. In cases where Member States had not signed and ratified Convention 108 'within a reasonable time' the European Commission reserved the right to propose the Council to adopt an instrument 'on the basis of the European Economic Community (EEC) Treaty'¹⁵⁹. Provided that the Convention 108 left '[...] open a large number of options for the implementation of the basic principles and at the beginning of the 90s it had been ratified by only seven Member States, of which one

¹⁵⁵ See Article (7)(a) of the Consolidated version of the 1992 Treaty of the European Community, *OJ C 224*, 31.8.1992, pp. 6-79 (1992 TEC hereinafter). The protection of personal data entered the EU scene to provide competitiveness for the European industry in the global IT market. In 1973, the European Commission advanced the proposal to build a community policy on data processing. This policy would be based on two fundamental points: firstly, the development of the capacities of European industry and, secondly, the promotion of the effective use of information. See the Communication from the Commission to the Council, Community policy on data processing, SEC(73) 4300 final, Brussels, 21.11.1973, p. 2.

¹⁵⁶ Hessische Datenschutzgesetz vom 7. oktober 1970 GVBl. II 300-10, *Gesetz-und Verordnungsblatt für das Land Hessen*, Part I, No. 41, 12.10.1970, available at www.starweb.hessen.de.

¹⁵⁷ Loi No. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée en dernier lieu par loi No. 2014-344 du 17 mars 2014, *Journal Officiel de la République Française*, 18.03.2014, available at www.legifrance.gouv.fr.

¹⁵⁸ Resolution of the Parliamentary Assembly No. 721 on *data processing and the protection of human rights*, Strasbourg, 1 February 1980. Thus, the European Community started inserting data protection principles in its pre-accession strategy while making express reference to the UN and/or the Council of Europe's frameworks. For an updated, compared analysis between the Council of Europe and the EU's regimes on personal data see Cécile de Terwangne, "Privacy and data protection in Europe: Council of Europe's Convention+ and the European Union's GDPR", in Gloria González Fuster, Rosamunde Van Berkel, and Paul De Hert, *Research Handbook on Privacy and Data Protection Law: Values, Norms, and Global Politics*, Cheltenham/Northampton, Edward Elgar Publishing, 2022, pp. 10-35.

¹⁵⁹ Commission Recommendation 81/679/EEC of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data, *OJ L 246*, 29.8.1981, p. 31.

still had no domestic legislation¹⁶⁰, the European Commission estimated that harmonisation was still needed to standardise the various degrees of protection granted to personal data among the Member States¹⁶¹.

Nevertheless, the European Community lacked a legal basis it could have relied on to legislate in the field of personal data and, even more importantly, it lacked any means by which to regulate human rights matters¹⁶². Consequently, the (then) new legislation on the protection of personal data was shaped under the logic of trade liberalisation among Member States¹⁶³. The European Commission presented an initial package of measures pursuing two main objectives: firstly, the enhancement of European industrial capacity and, secondly, the coordination of strategic sectors such as banking and telecommunications¹⁶⁴. Within this package a European Community legislative proposal on the protection of individuals with

¹⁶⁰ Commission Communication on the protection of individuals in relation to the processing of personal data in the community and information security, COM(90) 314 final, Brussels, 13.09.1990. Paul M. Schwartz, “European Data Protection Law and Restrictions on International Data Flows”, *Iowa Law Review*, No. 80, pp. 471-496, p. 478 ff., refers for example to the different legislations adopted by the Member States on transborder flows of personal data following the meagre indications given by Convention 108 on the matter.

¹⁶¹ Graham Pearce and Nicholas Platten, *op. cit.*, p. 531 ff.:

‘Spain ratified the Convention in 1984, but national legislation was not introduced until 1994, whilst Italy and Greece only introduced legislation in 1997. In Germany state and federal data protection laws had been instituted during the 1970s, while France had introduced a data protection law in 1978, a distinctive feature of which was the regulatory power given to the central supervisory authority (Commission Nationale d’Informatique et Libertés - CNIL). In the UK which, unlike the rest of the EC, has no general right of privacy, a Data Protection Act was introduced in 1984, but was restricted to automatic data processing, in accordance with Convention 108’.

¹⁶² Commission Communication on the protection of individuals in relation to the processing of personal data in the Community and information security, COM(90) 314 final, Brussels, 5.11.1990. See Diego Javier Liñán Nogueras, “Derechos Humanos y Unión Europea”, *Cursos Euromediterráneos Bancaja Derecho Internacional*, 2001, pp. 363-440, p. 374; Id., “Los derechos fundamentales en la Unión Europea”, in Araceli Mangas Martín and Diego Javier Liñán Nogueras, *Instituciones y Derecho de la Unión Europea*, Madrid, McGraw-Hill, 1996, pp. 581-596, pp. 13-16. Following his scholarship are, *inter alia*: Valentín Bou Franch and Mireya Castillo Daudí, *Derecho internacional de los derechos humanos y Derecho internacional humanitario*, Valencia, Tirant Lo Blanch, 2014, p. 195 ff., and Ana Salinas De Frías, *La Protección de los Derechos Fundamentales en la Unión Europea*, Granada, Comares, 2000.

¹⁶³ See Orla Lynskey, *The Foundations of EU Data Protection Law*, Oxford, Oxford Studies in European Law, 2015, pp. 47-48. The author highlights that the EU had no competence to enact the protection of rights established in its legislation and, therefore, the CJEU jurisprudence emphasised the integration market objective.

¹⁶⁴ With reason, the European Commission pointed out that, in the future, the real structure of the society may be branded by the way in which it would use information systems and it committed to present a program of proposals for the next year. The fear of being set apart from international trades was justified on the fact that the 90% of computers in Europe came from US and, among them, the 60% was monopolised by the International Business Machines Corporation. See the Communication from the European Commission to the Council, SEC(73) 4300 final, Brussels, 21.11.1973, p. 2.

regard to the processing of personal data dating back to 1990¹⁶⁵ was advanced¹⁶⁶ as part of the framework of the Common Commercial Policy (CCP)¹⁶⁷.

The proposal was soon amended because of the entry into force of the Maastricht Treaty that brought substantial changes to the previously envisaged procedure for making laws. In addition, the first proposal was too ambitious according to some of the Community's Member States that opposed high-level harmonisation legislation in favour of adhering to the minimalist approach laid out under Convention 108¹⁶⁸. The amended proposal was presented by the European Commission¹⁶⁹ on the basis of the approximation clause of Article 100a of the 1992 TEC¹⁷⁰, according to which the European Community could promote measures of approximation for the implementation of the internal market. Once again, the positive functionalist logic¹⁷¹ characterising the EU system of powers embedded in Article

¹⁶⁵ See the Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM(90) 314 final, *OJ C* 277, 5.11.1990, pp. 3-12, submitted by the European Commission on 27 July 1990. The proposal was initially based on Article 100a and Article 113 of the 1992 TEC regulating the harmonisation for the implementation of the internal market and the European commercial policy, but the latter was suppressed in the following version submitted by the European Commission, namely the Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(92) 422 final, Brussels, 15.10.1992. See the Commission Communication, COM(90) 314 final, Brussels, 13.09.1990.

¹⁶⁶ The Proposal was underpinned by Article 113 and Article 100a of the Treaty of the European Economic Community, *OJ L* 169, 29.6.1987, pp. 3-288, which required qualified majority voting within the Council without any participation of the European Parliament.

¹⁶⁷ Articles 113 and 100a of the Treaty establishing the European Economic Community, signed in Rome on 25 March 1957, entered into force on 1 January 1958 (TEEC): the former requiring the qualified majority voting in the Council, the latter the co-operation of the European Parliament.

¹⁶⁸ Graham Pearce and Nicholas Platten, *loc cit*.

¹⁶⁹ We should recall that Article 189a of the 1992 TEC foresaw that: '1. Where, in pursuance of this Treaty, the Council acts on a proposal from the Commission, unanimity shall be required for an act constituting an amendment to that proposal, subject to Article 189b(4) and (5). 2. As long as the Council has not acted, the Commission may alter its proposal at any time during the procedures leading to the adoption of a Community act'.

¹⁷⁰ List of proposals pending before the Council on 31 October 1993 for which entry into force of the Treaty on European Union will require a change in the legal base and/or a change in procedure, COM(93) 570 final, Brussels, 10.11.1993. Article 100a(1) of the 1992 TEC foresaw:

'1. By way of derogation from Article 100 and save where otherwise provided in this Treaty, the following provisions shall apply for the achievement of the objectives set out in Article 7a. The Council shall, acting in accordance with the procedure referred to in Article 189b and after consulting the Economic and Social Committee, adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market'.

José Martín y Pérez de Nanclares, 1997, *op. cit.*, p. 148, classifies it as a legal basis conferring the EU a 'general competence' and, for example, it was also used to adopt Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, *OJ L* 24, 30.1.1998, pp. 1-8.

¹⁷¹ Especially before the Lisbon Treaty when there was no systematisation of the EU competences. As José Martín y Pérez de Nanclares, *ibid.*, p. XVIII (our own translation), observed:

'[...] The Treaties, unlike the Constitutions of the federal and assimilated States or the 1984 Draft Treaty on European Union itself, do not contain a specific catalogue clearly defining the scope of Community action as opposed to that of the Member States. Nor do they regulate the question in the form

100a TEC – now Article 114 TFEU – justified the material expansion of the Community’s regulations while pursuing internal market objectives¹⁷². As Prof. de Witte underlines:

‘[i]nternal market legislation is always also ‘about something else’, and that something else may in fact be the main reason why the internal market measure was adopted’¹⁷³.

Therefore, the use of Article 100a by the European Commission was, in a certain way, to be expected; but what surprised was the fact that Member States did not contest it¹⁷⁴. The European Community could have been accused of circumventing the competential gap left by the founding Treaty and, consequently, the law-making procedure could have shifted to an unanimity vote inside of the Council¹⁷⁵; however, this did not happen. Prof. González Fuster notes that the European Commission justified its proposal on the questionable basis of ‘the necessity to avoid the surfacing of divergent, or conflicting, national laws [and] the ‘constitutional importance’ of the issue—despite the fact that by 1973 there were no

of subjects, as is also usual in federal Constitutions, but through objectives to be achieved, actions to be carried out and functions to be fulfilled. In short, it adopts a functional and teleological orientation’.

See also Léontin-Jean Constantinesco, “La naturaleza de las Comunidades Europeas”, in Manuel Díez de Velasco Vallejo, *El Derecho de la Comunidad Europea*, Madrid, Universidad Internacional Menéndez Pelayo, 1982, pp. 43-59, talking about a bivalent nature to highlight the coexistence of twofold objectives of integration and cooperation as well as twofold instruments on the internal market field and not.

¹⁷² Compare Luis Miguel Hinojosa Martínez, *El reparto de competencias entre la Unión Europea y sus Estados miembros*, Valencia, Tirant Lo Blanch, 2006, p. 55: ‘[...] the harmonisation of national laws to facilitate the functioning or establishment of the internal market should be seen as an explicit competence of the Community institutions, and not as a technique of “power grabbing”’ (our own translation). This clause would then differ from Article 352 TFEU – ex Article 308 of the Treaty establishing the European Community (Consolidated version 1997), *OJ C* 340, 10.11.1997, pp. 173-306 (1997 TEC hereinafter) and 235 of the TEEC –, the latter being a mechanism that does not fall within the theory of implied competences, as it proposes the attribution of new competences by means of a teleological interpretation of the Treaties (p. 44). In this sense, Article 114 TFEU itself is the main way in which non-approximation clauses have been undermined under the pretext of the completion of the internal market.

¹⁷³ See Bruno de Witte, “A competence to protect: The pursuit of non-market aims through internal market legislation”, in Philippe Syrpis, *The Judiciary, the Legislature and the EU Internal Market*, Cambridge, Cambridge University Press, 2012, pp. 25-46, p. 36.

¹⁷⁴ See for example C-209/97, *Commission of the European Communities v Council of the European Union*, 18 November 1999, EU:C:1999:559, paras. 33-37, where the CJEU found that Article 235 of the 1992 TEC was the correct legal basis instead of Article 100a of the 1992 TEC for the establishment of the Customs Information System (CIS):

‘Since Article 209a of the Treaty, in the version applicable when the contested regulation was adopted, indicated the objective to be attained but did not confer on the Community competence to set up a system of the kind at issue, recourse to Article 235 of the Treaty was justified [...] It is settled case-law that recourse to Article 100a is not justified where the measure to be adopted has only the incidental effect of harmonising market conditions within the Community’.

Also, the CJEU referred to the provisions of the CIS on the protection of personal data and considered that the potential harmonisation stemming from it should have been considered as ‘incidental effect of legislation’.

¹⁷⁵ Article 235 of the 1992 TEC, then Article 308 of the 1997 TEC, current Article 352 TFEU. According to the former:

‘If action by the Community should prove necessary to attain, in the course of the operation of the common market, one of the objectives of the Community, and this Treaty has not provided the necessary powers, the Council shall, acting unanimously on a proposal from the Commission and after consulting the European Parliament, take the appropriate measures’.

constitutional provisions on data processing in any European country (yet)¹⁷⁶ and that because certain Member States had still not adopted any form of data protection laws¹⁷⁷. Italy's first legislative text regulating the protection of personal data was adopted following the DPD in 1996¹⁷⁸, though a fundamental right to the protection of personal data was consecrated only in 2003¹⁷⁹. However, rather than questioning why the Union chose to undertake a "preventive" action, which the CJEU had justified on other occasions¹⁸⁰, the question should rather have been whether the objective pursued by the European Commission was related to common market or human rights issues since, in the latter case, the European Community would have exceeded its powers¹⁸¹. Referring to Article 100a, the European Community was legislating in a field where the approximation clause¹⁸² did not suit the *statu quo ante* – at least as far as some Member States, those that lacked their own normative text, were concerned. Profiting of the legal uncertainties caused by the lack of a clear competence catalogue and of rules governing its exercise, the '[...] Community law-

¹⁷⁶ Gloria González Fuster, *op. cit.*, p. 112.

¹⁷⁷ The intervention of the EU through a regulation approximating Member States' legislation goes back to the positive integrationist strategy that have been enabling the establishment and functioning of an internal market project since this was envisaged in the Single European Union Act of 1986 – see Robert Schütze, *European Union Law*, Cambridge, Cambridge University Press, 2018, pp. 549-587.

¹⁷⁸ Legge 31 dicembre 1996, No. 675, Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, *Gazzetta Ufficiale* No. 5 del 08.01.1997. Spain, instead, adopted the Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, *Boletín Oficial del Estado* No. 298, 14.12.1999, as a transposition of the European Community's legislation revising the previous Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), *Boletín Oficial del Estado* No. 262, 31.10.1992. An in-deep analysis is given by Gloria González Fuster, *op. cit.*, p. 147 ff., where she stands out that some Member States lacked an own legislation while other ones had to adapt it to the DPD.

¹⁷⁹ Decreto Legislativo 30 giugno 2003, No. 196, Codice in materia di protezione dei dati personali, ((recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) No. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE)), *Gazzetta Ufficiale* No. 174, 29.7.2003, and Giusella Finocchiaro, *Privacy e protezione dei dati personali: Disciplina e strumenti operativi*, Bologna, Zanichelli, 2012, p. 1 ff.

¹⁸⁰ Among others, T-526/10, *Inuit Tapiriit Kanatami, Nattivak Hunters and Trappers Association, Pangnirtung Hunters' and Trappers' Association, Jaypootie Moesiesie, Allen Kooneeliusie, residing in Qikiqtarjuaq, Toomasie Newkingnak, David Kuptana, Karliin Ariak, Canadian Seal Marketing Group, Ta Ma Su Seal Products, Fur Institute of Canada, NuTan Furs, Inc., GC Rieber Skinn AS, Inuit Circumpolar Council Greenland (ICC-Greenland), Johannes Egede, Kalaallit Nunaanni Aalisartut Piniartullu Kattuffiat (KNAPK), William E. Scott & Son, Association des chasseurs de phoques des Îles-de-la-Madeleine, Hatem Yavuz Deri Sanayi iç Ve Diş Ticaret Ltd Şirketi, Northeast Coast Sealers' Co-Operative Society, Ltd, v European Commission*, 25 April 2103, EU:T:2013:215, para. 31.

¹⁸¹ C-376/98, *Federal Republic of Germany v European Parliament, and Council of the European Union*, 5 October 2000, EU:C:2000:544. For a critic, see Carlos Ruiz Miguel, "El derecho a la protección de datos personales en la carta de derechos fundamentales de la Unión Europea: Análisis crítico", *Revista de Derecho Comunitario Europeo*, No. 14, 2003, pp. 7-43, p. 20 ff.

¹⁸² In this sense, Article 114 TFEU uses the term 'approximation' as a synonym of 'harmonisation' as confirmed by its fourth paragraph.

making procedures were the key not only for the inter-institutional relations and institutional balance, but also for the definition and the development of the system of competences¹⁸³.

Article 100a as a legal basis enabled the adoption of the DPD under the cooperation procedure of Article 189b of the 1992 TEC¹⁸⁴. The cooperation procedure had recently empowered the European Parliament to take part in the law-making process together with the Council¹⁸⁵ and the more accommodating approach undertaken by the European Commission in its amended Proposal was decisive to the creation of a common data protection legislation. According to Prof. González Fuster:

‘[...] Mediterranean countries and the Benelux were particularly supportive, whereas the UK and Ireland opposed the very idea of harmonising the field with a Directive. Germany appeared as undecided. [...] Eventually, Germany joined the British, Irish and the also unconvinced Danish delegation to support a joint document against the Proposal’¹⁸⁶.

Nevertheless, due to the reluctance of a few Member States, to which must be added the strong objections by private companies¹⁸⁷, trialogue¹⁸⁸ negotiations were required to overcome the political impasse. The German green light that (apparently¹⁸⁹) renounced to a *de minimis* regulation while opting for ‘secure harmonisation’ left the United Kingdom as the sole opponent¹⁹⁰.

¹⁸³ Teresa Fajardo del Castillo, *La política exterior de la Unión Europea en materia de medio ambiente*, Madrid, Tecnos, 2005, pp. 28-29 (the translation is ours).

¹⁸⁴ Notably, the Opinion of the Commission pursuant to Article 189b(2)(d) of the EC Treaty, on the European Parliament’s amendments to the Council’s common position regarding the proposal for a European Parliament and Council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(95) 0375 final, Brussels, 18.07.1995, issued a positive opinion on the few amendments brought by the European Parliament. Although Article 289b(3) of the 1992 TEC allowed the Council to approve them on a qualified majority, but from the information available at www.eur-lex.europa.eu the ‘Approval by the Council of the EP amendments at 2nd reading’ followed the unanimity decision mode.

¹⁸⁵ Article 100a evolved in Article 95 of the 1997 TEC, and in current Article 114 TFEU. Although the European Commission launched the first supranational impetus in the ‘70s – e.g., Communication by the Commission of the European Communities concerning a Community policy for data processing, Brussels, SEC(73) 4300, Brussels, 21.11.1973 – the European Parliament had always pressured to empower the Community with a data protection law – see Didier Bigo, Sergio Carrera, Gloria González Fuster, Elspeth Guild, Paul de Hert, Julian Jeandesboz, and Dr Vagelis Papakonstantinou, *Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament*, Policy department C: Citizens’ rights and constitutional affairs civil liberties, justice and home affairs, Brussels, 2011.

¹⁸⁶ Gloria González Fuster, *op. cit.*, p. 128.

¹⁸⁷ A detail analysis is given by Graham Pearce and Nicholas Platten, *op cit.*, pp. 534 and 355.

¹⁸⁸ Common Position (EC) No 1/95 adopted by the Council on 20 February 1995 with a view to adopting Directive 95/. . ./EC of the European Parliament and of the Council of . . . on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ C* 93, 13.4.1995, pp. 1-24.

¹⁸⁹ See further Chapter 2.

¹⁹⁰ The United Kingdom tried to undermine the majority achieved in a questionably way before the principle of sincere cooperation and left the Council one step away from unanimity. See Alison White, “Control of Transborder Data Flow: Reactions to the European Data Protection Directive”, *International Journal of Law and Information Technology*, Vol. 5, No. 2, 1997, pp. 230-247, p. 238:

2.1. The limits to the first internal market directive on the protection of personal data

Despite carrying on an ‘internal market facet’¹⁹¹, the DPD achieved the introduction of a human rights dimension by referring to Convention 108¹⁹². Making the supranational order supersede the Member States’ laws as far as the protection of their citizens’ personal data was concerned was justified in the light of the Member States’ commitments *vis-à-vis* international law¹⁹³. Therefore, the legislation on the protection of personal data – but not Convention 108 – was designed on the basis of a complex relationship between safeguarding the individual’s right to a private and family life¹⁹⁴ on one hand, and, on the other, the need to exchange information within Member States for economic reasons¹⁹⁵. Specifically, the DPD pursued two main objectives: first, it aimed at protecting fundamental rights and freedoms of individuals, especially the right to privacy; second, it forbade any restrictions to the ‘free flow’ of personal data¹⁹⁶. Unlike the Council of Europe’s Convention 108, that only

‘As with all compromises no one is entirely happy. The UK Government has made it clear that it does not consider the Directive to be necessary and would, through choice, have preferred to achieve harmonisation by forcing Italy and Greece, the only Member States without data protection statutes, to enact legislation based upon the Council of Europe Convention. 24 It has also stated that it intends to amend the DPA only to the minimum extent necessary to fulfil its European commitments’.

¹⁹¹ Gloria González Fuster, *op. cit.*, p. 126.

¹⁹² Recital (11) DPD. Peter Hustinx, “EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation”, in Marise Cremona, *New Technologies and EU Law*, Oxford, Oxford University Press, 2017, pp. 123-173, p. 139:

‘Directive 95/46/EC has used Convention 108 as a starting point for the harmonization of data protection laws in the EU, and specified it in different ways. This involved the substantive principles of data protection, the obligations of controllers, the rights of data subjects, and the need for independent supervision as main structural elements of data protection. However, the nature of data protection as a system of ‘check and balances’ to provide protection whenever personal data are processed was not changed. In other words, Article 7 and 8 do not have the same character and must be clearly distinguished’.

Graham Pearce and Nicholas Platten, *op. cit.*, p. 533, highlights that the DPD ‘[...] restated the arguments in favour of a common approach to data protection, but the text was restructured with the fundamental and more familiar provisions of the Council of Europe Convention being given greater prominence’.

¹⁹³ Still the Costituzione della Repubblica Italiana, *Gazzetta Ufficiale* No. 298, 27.12.1947, for example, does not dedicate a specific Article to the right to the protection of personal data. Its protection has been interpreted jurisprudentially based on other Articles that are manifestations of it – namely, Articles 13, 14, 15, 21, and 29. However, the specificities stemming from the former makes scholars arguing that the “open clause” of Article 2 of the Italian Constitution should be chosen in order to give birth to a new fundamental right – see Giulia Tiberi, *loc. cit.*

¹⁹⁴ See *supra*.

¹⁹⁵ See Article 1(2) DPD specifying that ‘Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1’.

¹⁹⁶ Marc Rotenberg and David Jacobs, “Updating the Law of Information Privacy: The New Framework of the European Union”, *Harvard Journal of Law & Public Policy*, No. 36, 2013, pp. 605-652, p. 617:

‘In setting up this framework, the EU Data Protection Directive refers to Article 8 of the European Convention on Human Rights, and its classification of privacy rights, as “fundamental” 6 and states that the Directive’s purpose is to promote data sharing while protecting the principles espoused in that Convention? The Directive thus achieved the twin goals of promoting the internal market with clear standards for data transfers and simultaneously safeguarding a fundamental right’.

referred to the automatic processing of ‘information relating to an identified or identifiable natural person’¹⁹⁷, the DPD focused on a wider spectrum of data flows by also including manual processing used in filing systems¹⁹⁸, a regime on the transfer of personal data to third countries¹⁹⁹, and the provision of an independent supervisory authority ensuring its correct implementation²⁰⁰.

However, the safeguard of a fundamental right to the protection of personal data could have never become the prominent objective of the DPD, as the organisation’s legal *raison d’être* was to contribute to the internal market. In addition, the DPD would have been invalidated because of the EU’s lack of power to enact fundamental rights legislation. In *Rundfunk*, Advocate General Tizzano firmly maintained that:

‘If, furthermore, over and above the purpose of encouraging the free movement of personal data within the internal market, one also attached to the Directive the additional, independent objective of guaranteeing the protection of fundamental rights (in particular the right to privacy), there would be a danger of compromising the validity of the Directive itself, because, in such a case, its legal basis would clearly be inappropriate. Article 100a could not be invoked as a basis for measures going beyond the specific purposes stated in that provision, that is to say, for measures not justified by the objective of encouraging ‘the establishment and functioning of the internal market’²⁰¹.

¹⁹⁷ Article 2(a) DPD. A borderline between the concepts of ‘personal data’ and information was roughed out in C-141/12 and C-372/12, *YS v Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v M. S.*, 17 July 2014, EU:C:2014:2081, where, before the request of a third country national to access the minutes containing the reasoning founding the approval or refusal of a resident permit, the CJEU affirmed that the applicant’s name, date of birth, nationality, gender, ethnicity, religion, and language would be considered as personal data in the light of the DPD, but the legal analysis contained in the minutes fell outside this definition, even if this contained personal data. In C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, 19 October 2016, EU:C:2016:779, the CJEU sentenced that an Internet Protocol dynamic address enabling to consult German federal services’ webpages should have been considered as identifying, directly or indirectly, the user provided that the Federal Republic of Germany could aggregate the information already held by it and the one stored by the user’s internet service provider, then, the Internet Protocol dynamic address should have been considered as ‘personal data’.

¹⁹⁸ Recital (27) DPD: ‘[...] whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data’ which excludes unstructured files. As a consequence, some Member States also extended the scope of that Convention 108 to personal data processed by non-automated means – see, for example, the Italian Declaration on Article 3(2)(c), sent by latter dated the 28 March 1997 to the Council of Europe available at www.coe.int: ‘Italy declares, with regard to Article 3, paragraph 2, sub-paragraph c, of the Convention, that it will also apply the Convention to data classified without the aid of electronic or automatic processing’.

¹⁹⁹ Chapter IV DPD.

²⁰⁰ Article 28 DPD.

²⁰¹ See the Opinion of Advocate General Tizzano, C-465/00, *Neukomm and Lauremann v Österreichischer Rundfunk*, 14 November 2002, EU:C:2002:662, para. 54, recalling its previous opinion in C-101/01, *Bodil Lindqvist v Åklagarkammaren i Jönköping*, 19 September 2002, EU:C:2002:513, para. 42:

‘Also, as Mrs Lindqvist has pointed out, if in addition to the aim of encouraging the free movement of personal data in the internal market, the Directive were held to have other, independent, objectives connected with social imperatives and the protection of fundamental rights (in particular the right to privacy), the very validity of the Directive might be called into question, since in that case its legal basis would be manifestly inadequate. Article 100a could not be cited as a basis for measures that went beyond

The bottom-down approach through which the European Community was incorporating data protection principles in the Member States' legal systems, was preventing the CJEU from imposing the respect of the correspondent right while implementing European Community law. At that time, and at the European Community level, the protection of individuals' fundamental rights was guaranteed only by virtue of the CJEU jurisprudence as general principles of the European Community's legal order that could bind Member States to adhere to them while implementing or derogating European Community law²⁰². In a period when the CJEU was still hesitant to create rulings regarding fundamental rights – including the right to a private and family life²⁰³ – the scope of the European Community powers regarding the protection of personal data was shaped along the logic of trade liberalisation among Member States²⁰⁴. In analysing the earliest pronouncements, Prof. Lynskey highlights that the interpretation of the dispositions of the DPD was leaving too broad a margin of appreciation for national legislations and that '[t]hese disparities, lead to fragmentation and are inimical to the objectives of the Directive. It can be seen that the Court's reluctance to assert the fundamental rights underpinning the Directive endangered the coherence of its internal market objective which had been so keen to promote in earlier cases'²⁰⁵. Had the EU wanted to safeguard the necessity of circulating the information within the internal market, the right to the protection of personal data had to be integrated into the Member States' legal orders²⁰⁶. As Prof. Salerno teaches:

'[...] the growing importance of the international organisation and its direct contact with the private individual must go hand in hand with the expansion of the human rights it protects. [...] it is only if the rights of liberty and democracy are already rooted in the domestic law of countries that are members of an organisation that it is possible to foster

the specific aims mentioned in that provision, that is to say measures that were not justified by the objective of encouraging the establishment and functioning of the internal market'.

²⁰² See Diego Javier Liñán Nogueras "Derechos humanos y libertades fundamentales en la Unión Europea" in Araceli Mangas Martín and Diego Javier Liñán Nogueras, *loc. cit.* Specifically, the CJEU admitted the possibility that fundamental rights constituted common traditions among the Member States or that these were all bound by an international human rights instruments – which is known as the doctrine of incorporation – see C-29/69, *Stauder v Stadt Ulm*, 24 June 1969, EU:C:1969:27; C-11/70, *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel*, 17 December 1970, EU:C:1970:114; C-4/73, *Nold KG v Commission*, 14 May 1974, EU:C:1974:51, and C-260/89, *ERT v DEP*, 18 June 1991, EU:C:1991:254.

²⁰³ Article 1(1) DPD that specifically refers to the '[...] right to privacy with respect to the processing of personal data'.

²⁰⁴ See Orla Lynskey, 2015, *op. cit.*, pp. 47-48. The author highlights that the EU had no competence to enact the protection of rights established in its legislation and, therefore, the CJEU jurisprudence emphasised the integration market objective.

²⁰⁵ *Ibid.*, pp. 57-58.

²⁰⁶ Following the proposal of inserting a specific Article on personal data in the Nice Charter, the Recommendation of the Article 29 DPWP No. 4/99 on *the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights*, Brussels, 7.09.1999, p. 2, expressed its favorable opinion underlining that '[...] some European countries have incorporated fundamental rights on data protection into their constitution. In others, these rights have acquired constitutional force through case law'.

their development in the sphere of international organisations. This brings us back to the fundamental dilemma of internationalist doctrine, namely whether to push the affirmation of human rights to the point of ‘no return’ for the freedom of states in the international order²⁰⁷.

2.2. A fundamental (human?) right to the protection of personal data

A first step toward the codification²⁰⁸ of DPD’s principles was made in 1999 when the European Community’s institutions and bodies were bound to the Community’s data protection framework²⁰⁹. According to Article 286 of the 1997 TEC:

‘1. From 1 January 1999, Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty.

2. Before the date referred to in paragraph 1, the Council, acting in accordance with the procedure referred to in Article 251, shall establish an independent supervisory body responsible for monitoring the application of such Community acts to Community institutions and bodies and shall adopt any other relevant provisions as appropriate’.

Article 286(1) of the 1997 TEC was concretised by Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by Community institutions and bodies and on the free movement of such data²¹⁰ (ECDPR). The ECDPR established the EDPS²¹¹ and, in a departure from the DPD’s approach, it also regulated the confidentiality

²⁰⁷ Francesco Salerno, “Bobbio, i diritti umani e la dottrina internazionalista italiana”, *Diritti Umani e Diritto Internazionale*, No. 3, 2009, pp. 485-582, p. 501 ff. (our own translation).

²⁰⁸ Paola Mori, “Gli strumenti della codificazione nel diritto dell’Unione Europea”, in Alessandra Annoni, Serena Forlati, and Francesco Salerno, *La codificazione nell’ordinamento internazionale e dell’Unione europea*, Napoli, Editoriale Scientifica, 2019, pp. 301-369, p. 236: ‘The Charter came into being outside the system of Treaties, by means of a very special procedure and an act of undefined legal value, and was only able to express its full normative potential by amending the Treaties’ (our own translation).

²⁰⁹ Francesco Maiani, “Le cadre réglementaire des traitements de données personnelles effectués au sein de l’Union européenne”, *Revue Trimestrielle de Droit Européenne*, No. 2, pp. 283-309, p. 289 (our own translation):

‘[...] by making applicable to the institutions and bodies the acts originally designed to harmonise national laws, the idea was to make the level of protection in the Member States and within the European Community equivalent and thus eliminate any obstacle to the transmission of data between national and Community administrations’.

The possibility to tie the European Community institutions before the Member States themselves had already explored with regards to the respect of human rights under European Community Law – confront Article F(2) of the Treaty on European Union, *OJ C* 191, 29.7.1992, pp. 1-112 (1992 TEU hereinafter) and the C-36/75, *Roland Rutili v Ministre de l’intérieur*, 28 October 1975, EU:C:1975:137, commented by Sionaidh Douglas-Scott, “The European Union Fundamental Rights”, in Robert Schütze and Takis Tridimas, *Oxford Principles of European Union law. Vol. I: The European Union Legal Order*, Oxford, Oxford University Press, 2018, pp. 383-422, p. 411.

²¹⁰ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, *OJ L* 8, 12.1.2001, pp. 1-2, see its Article 2.

²¹¹ Articles 1(2) and 41-48 ECDPR.

of communication within EU institutions and bodies²¹² in order to put them on an equal footing with States' administrations, which were bound to the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive)²¹³. However, the ECDPR did not replace either the DPD or the other sectoral instruments that had been adopted by the European Community as Article 286(1) of the 1997 TEC made them applicable to the institutions and bodies. Their relationship, then, was underpinned by the principle of *lex specialis derogat generali*, where the ECDPR was the special legislation and the DPD the general framework²¹⁴.

A specific fundamental right on the protection of personal data was proclaimed on 7 December 2000 with the Treaty of Nice²¹⁵. According to the proclamation:

- '1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority'.

Despite some Member States' reluctance to grant the right to the protection of personal data from the one of privacy²¹⁶, '[t]he assertion according to which data protection was an element of privacy disappeared'²¹⁷. Therefore, the Nice Charter finally distinguished the right to the protection of personal data as separate to the right to a private and family life – Articles 7²¹⁸ and 8 respectively – while recognising the European Community's leading role over not only other international organisations that were already providing a protective

²¹² Chapter IV ECDPR.

²¹³ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *OJ L* 201, 31.7.2002, pp. 37-47.

²¹⁴ Francesco Maiani, *op. cit.*, p. 294 ff.

²¹⁵ See the Treaty of Nice amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, *OJ C* 80, 10.3.2001, pp. 1-87. Gloria González Fuster, *op. cit.*, p. 186 ff., well explains that any previous attempts to draft a Bill of Right for the Community did not make direct reference to the right to protect personal data but to the one of privacy, secret communication, or access to information.

²¹⁶ Among which Germany, The Netherlands, Sweden, and Italy's representatives in the 'Convention' in charge of drafting the Charter. See, *inter alia*, the Praesidium Note in Council of the EU, *Subject: Draft Charter of Fundamental Rights of the European Union— Amendments submitted by the members of the Convention regarding civil and political rights and citizens' rights (Reference document: CHARTE 4284/00 CONVENT 28 (REV 1 in French only), (oR. multilingual), CHARTE 4332/00, CoNVENT 35, Brussels, 25 May 2000.*

²¹⁷ Gloria González Fuster, *op. cit.* p. 197.

²¹⁸ According to it: 'Everyone has the right to respect for his or her private and family life, home and communications'.

framework to individuals' personal data²¹⁹, but also over some of the Member States' constitutional legal orders that did not recognise an *ad hoc* fundamental right²²⁰. In these terms, the CFREU was deemed not merely to "reaffirm"²²¹ the right, but to be founding a new fundamental right on the protection of personal data 'in the light of changes in society, social progress and scientific and technological developments'²²². As Prof. González Fuster states:

'It is certainly rooted in previously existing instruments. It innovates to the extent that it establishes that the elements mentioned deserve to be protected as elements of a fundamental right deserving protection per se [...], and that the protection is not exclusively granted to data in a way or another related to the right to respect for private life, but to personal data in general. In this sense, it goes beyond the scope of the protection granted on the basis of the ECHR, and of the common constitutional traditions of the member States [...]'²²³.

Thus, at the beginning of the 2000s, data protection rights were imposing obligations to European Community institutions while softly guaranteeing rights to individuals²²⁴ and speeding up the integration of Member States' legislations²²⁵. The CJEU started releasing wide interpretations of the DPD's norms which made the fundamental right facet evident alongside the market liberalisation one. In *Lindqvist*, the CJEU sentenced that to fall within the scope of the DPD, data processing activities should have not necessarily been seen as

²¹⁹ See Franziska Boehm, *op. cit.*, pp. 19-173.

²²⁰ See *supra*.

²²¹ Declaration concerning the Charter of Fundamental Rights of the European Union, *OJ C* 326, 26.10.2012, p. 339.

²²² Gloria González Fuster, *op. cit.*, p. 198. Hielke Hijmans, *The European Union as Guardian of Internet Privacy*, Cham, Springer, 2016, pp. 185-26, recaps that different classification had been made to systematise human rights: first, a positive method would delimit the rights on the basis of the Charter's dispositions; second, a nature-based definition leverages on common values – e.g., human dignity or autonomy – and, third, the historical method differentiates civil and political rights from social rights which is also reflected in the first/second generation dichotomy. The author also advances his own taxonomy made of six groups of rights where Article 8 of the CFREU would fall within those fundamental rights that relevant for human dignity, though non-absolute. Article 8 CFREU could then fall within the fourth generation of human rights, that mushroom in the international debate following new technologies challenges, according to the classification made, for example, by: María Eugenia Rodríguez Palop, *La nueva generación de derechos humanos: origen y justificación*, Madrid, Dykinson, 2018, or Javier Bustamante Donas, "Segundos pensamientos. La cuarta generación de derechos humanos en las redes digitales", in Paloma Llaneza, *TELOS 85: Los derechos fundamentales en Internet*, Madrid, Fundación Telefónica, 2010, pp. 81-89. However, this would remain a mere descriptive systematisation that does not reveal what is the real range of the states' obligations – see Riccardo Pisillo Mazzeschi, *op. cit.*, p. 136.

²²³ Gloria González Fuster, *op. cit.*, p. 205.

²²⁴ Hielke Hijmans and Alfonso Scirocco, "Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to help?", *Common Market Law Review*, Vol. 46, 2009, pp. 1485-1525, p. 1487.

²²⁵ On the instrumentalisation of fundamental rights as a tool of integration see Jason Coppel and Aidan O' Neill, "The European Court of Justice: taking rights seriously", *Common Market Law Review*, Vol. 29, No. 4, 1992, pp. 669-692, as well as José Martín y Pérez de Nanclares, "The protection of human rights in the European Union", in Felipe Gómez Isa and Koen de Feyter, *op. cit.*, pp. 777-802, p. 778. The authors defend that the CJEU passed from a defensive to an offensive use of fundamental rights to expand its jurisdiction in area reserved to the Member State sovereign competences.

having a direct link with the fundamental freedoms of the internal market²²⁶. Only activities strictly excluded from the scope of the DPD²²⁷ should have been set aside from the range of the EU action such as, for example, so-called ‘domestic activity’²²⁸. In its reasoning, the Luxembourg Court relied on the international instruments – and, especially, on those of the Council of Europe – that were already binding the Member States as ‘general principles of the law of the Communities’. However, the CJEU has progressively emancipated itself from international human rights instruments – including Article 8 of the ECHR – as Article 8 of the CFREU in fact codified its own set of principles and rights to protect personal data used in processing activities rather than the individual’s right to privacy²²⁹.

- The principle of fairness is ‘[...] an overarching principle which requires that personal data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject’²³⁰ and it is usually associated with the good faith requirement²³¹ ensuring accountability of the data controller *vis-à-vis* the individual.

²²⁶ C-101/01, *Bodil Lindqvist v Åklagarkammaren i Jönköping*, para. 42.

²²⁷ See Article 3(2) DPD.

²²⁸ *Ibidem*. In the EDPS perspective, controllers or processors that provide the services for such a personal or household activity which, in includes cloud services for consumers, are included – confront the Opinion of the EDPS on the Commission’s Communication on “Unleashing the potential of Cloud Computing in Europe”, Brussels, 16.11.2012, p. 9 (when not specified otherwise, the EDPS documents are available in its official webpage at www.edps.europa.eu). This exception is also reflected in some of the declarations made by the Member States to the Convention 108 on inhouse activities – see the Italian Declaration on Article 3(2)(a), sent by latter dated the 28 March 1997 for which it excluded automated personal data files concerning ‘[p]rocessing of personal data carried out by individuals exclusively for personal purposes, provided that these data are not intended for systematic communication of for broadcast’.

²²⁹ We might recall its position in the historical judgment C-203/15 and C-698/15, *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, 21 December 2016, EU:C:2016:970, paras. 127 and 129:

‘As a preliminary point, it should be recalled that, whilst, as Article 6(3) TEU confirms, fundamental rights recognised by the ECHR constitute general principles of EU law, the ECHR does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into EU law [...] It should be added, finally, that Article 8 of the concerns a fundamental right which is distinct from that enshrined in Article 7 of the Charter and which has no equivalent in the ECHR’.

Similarly, the Article 29 DPWP affirmed that the DPD covered data processing activities outside home and family, such as labour law, criminal convictions, administrative sanctions or judgments in civil cases. See the Opinion of Article 29 DPWP No. 4/2007 on the concept of personal data, Brussels, 20.06.2007, p. 7.

²³⁰ Guidelines of the Article 29 DPWP No. 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0, Brussels, 20.10.2020, pp. 17-18; Winston J. Maxwell, “Principles-based regulation of personal data: the case of ‘fair processing’”, *International Data Privacy Law*, 2015, Vol. 5, No. 3, pp. 205-216, and Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen Borgesius, “The European Union general data protection regulation: what it is and what it means”, *Information & Communications Technology Law*, Vol. 28, No. 1, 2019, pp. 65-98, p. 77.

²³¹ Damian Clifford, and Jef Ausloos, “Data Protection and the Role of Fairness”, *Yearbook of European Law*, Vol. 37, 2018, pp. 130-187.

- The principle of limited purposes for data processing requires data to be processed for specified, explicit, and legitimate purpose/s²³²; specifically, in the case of systems storing personal data, a shift in the usage of the data for purposes other than the one initially envisaged is commonly known as ‘function creep’²³³. Yet further processing is not forbidden if the first purpose pursued is respected – this principle is also known as compatible use²³⁴.
- The principle of lawfulness establishes on which grounds personal data can be processed and, here, the CFREU brings together²³⁵ two different scholarly approaches – those of self-determination²³⁶ and the non-consent²³⁷ – while relying on both the consent²³⁸ of the person concerned and on some other legitimate basis laid down by law²³⁹.

²³² Opinion of the Article 29 DPWP No. 03/2013 on *purpose limitation*, Brussels, 2.04.2013: specific, since the purpose shall be sufficiently defined so as to implement the necessary data protection safeguards and to delimit the scope of the processing; explicit means that the purpose must be ‘sufficiently unambiguous and clearly expressed’, and ‘legitimate’ demands the respect of the law including the principle of lawful processing.

²³³ *Ibid.*, p. 21. In C-543/09, *Deutsche Telekom AG v Bundesrepublik Deutschland*, 5 May 2011, EU:C:2011:279, para. 65, the CJEU maintained that when the data subject is assigned a telephone number according to the ePrivacy Directive, the acceptance of its publication in printed or electronic directories available to the public can be also extended to the transfer of data to a third party undertaking that they intend to publish such data for the same purposes. Nevertheless, the CJEU also specified that the subscriber should have been duly informed, before the first inclusion of their data in a public directory, of the purpose of that directory, and of the fact that those data may be communicated to another telephone service provider.

²³⁴ See *infra*.

²³⁵ As Herke Kranenborg, “Article 8: Protection of Personal Data”, in Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward, *The EU Charter of Fundamental Rights: A Commentary*, Oregon, Hart Publishing, 2014, pp. 223-266, p. 229, affirms that, although the right to the protection of personal data is based on the self-determination principle of the data subject consent, EU law clearly opens the way to other forms of legitimate processing of personal data which shifts the focus of its protection to the provision of checks and balances in case of non-consent lawful processing.

²³⁶ Interpreting the right to data processing as a restriction to the corresponding fundamental right for which purpose the individual shall be empowered to take control over it are Gloria González Fuster and Serge Gutwirth, “Opening up personal data protection: a conceptual controversy”, *Computer Law & Security Review*, No. 29, 2013, pp. 531-539.

²³⁷ Supporting the idea that data protection does not aim at preventing the processing of personal data so that the individual’s consent is only one of the legitimate bases for processing are: Peter Hustinx, “EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation”, *Collected Courses of the European University Institute’s Academy of European Law: 24 Session on European Union Law*, 2013, pp. 1-52, available at www.edps.europa.eu; Lisa M. Austin, “Enough About Me: Why Privacy is About Power, not Consent (or Harm)”, in Austin Sarat, *A World Without Privacy: What Law Can and Should Do?*, New York, Cambridge University Press, pp. 131-189, and Raphael Gellert and Serge Gutwirth, *loc. cit.*, affirming that “data protection by default” accepts data processing.

²³⁸ Note that the consent is presumed not to be freely given also when it is related to multiple data processing operations ‘[...] despite it being appropriate in the individual case’ according to C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH*, 1 October 2019, EU:C:2019:801, para. 62. Historically is the CJEU jurisprudence on the consent of the data subject surfing on the internet: see C-61/19, *Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*, 11 November 2020, EU:C:2020:901.

²³⁹ In C-439/19, *B and Latvijas Republikas Saeima*, 22 June 2021, EU:C:2021:504, for example, the CJEU found the Latvian law authorising the disclosure to the public or economic operators by the Latvian Road Safety Directorate of personal data relating to penalty points to any person disproportionate in the light of the objective of improving road safety pursued. In C-73/16, *Peter Puškár v Finančné riaditeľstvo Slovenskej*

- The right of access²⁴⁰ to data that has been collected concerning the individual, and the right to have it rectified²⁴¹. The former allows the data subject to know whether his/her personal data has been processed; the latter ensures that the data stored is reliable and, if necessary, updated – i.e., accurate²⁴².
- The control by an “independent” – both internally and externally²⁴³ – authority in charge of ensuring compliance with rules on the protection of personal data and their free movement²⁴⁴.

Despite this set of core principles, their relationship between the right to the protection of personal data and the right to privacy remains an open field of research²⁴⁵. Hustinx, for example, affirms that the right to the protection of personal data is both broader and more limited than right regarding privacy: on the one hand, Article 8 CFREU may concern other fundamental rights and freedoms; on the other hand, data protection only relates to the processing of information without considering other aspects the concept of privacy would include²⁴⁶. The CJEU itself recognises that the right to privacy represents a valuable tool

republiky and Kriminálny úrad finančnej správy, 27 September 2017, EU:C:2017:725, the CJEU was asked whether the processing of personal data consisting in the drafting of a list of persons by the Finance Directorate and the Financial Administration Criminal Office (Slovakia) was necessary for reasons of public interest as it was directed at combating tax fraud. Yet, the Court gave no answer and referred to the national judge to assess whether the contested list respected the proportionality principle.

²⁴⁰ In C-141/12 and C-372/12, *YS v Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v M. S.*, the CJEU maintained that third country nationals shall be recognised the right to access the personal data contained in the minutes justifying the approval or the refusal of a resident permit.

²⁴¹ C-434/16, *Peter Nowak v Data Protection Commissioner*, 20 December 2017, EU:C:2017:994, paras. 25 and 57.

²⁴² *Ibidem*.

²⁴³ The former refers to the so-called ‘functional independence’ for which national supervisory authorities shall not receive any instruction while exercising their functions; the latter excludes any form of direct/indirect external influence – see C-518/07, *European Commission v Federal Republic of Germany*, 9 March 2010, EU:C:2010:125, and C-614/10, *European Commission v Austria*, 16 October 2012, EU:C:2012:125.

²⁴⁴ The CJEU maintains that their designation shall prevent any direct or indirect influence in the decision-making process deployed in the exercise of their functions – T-115/13, *Gert-Jan Dennekamp v European Parliament*, 5 July 2015, EU:T:2015:497.

²⁴⁵ Some scholars maintain that the right to a private and family life has a wider scope than the right to the protection of personal data if it is estimated that it includes, among others, the right to be let alone or the right to develop personal relationship with each other – see Franziska Boehm, *op. cit.*, p. 4. However, the right to the protection of personal data can be perceived as being wider than the right to a private and family life in the light of the huge definition conferred by the EU legislation to ‘personal data’ – in this sense see Juliana Kokott and Christoph Sobotta, “The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR”, *International Data Privacy Law*, Vol. 3, No. 4, 2013, pp. 222-228. Matteo E. Bonfanti, *op. cit.*, p. 441 ff., maintains that a middle way consists in defining their relationship as ‘twins but not identical’, while Irene Kamara, *Data Protection Standardisation: The role and limits of technical standards in the European Union data protection law*, The Netherlands, Tilburg University/Vrije Universiteit Brussel, 2021, p. 4, affirms that ‘[...] the difference lies with their scope and formulation. Namely, that the right to respect for private life constitutes ‘general prohibition on interference’, while the protection of personal data is a ‘system of checks and balances to protect individuals whenever their personal data is processed’.

²⁴⁶ Peter Hustinx, 2017, *op. cit.*, pp. 123-173, p. 127.

when Article 8 of the CFREU cannot be applied²⁴⁷, for example, when the definition of ‘personal data’ is not met. In *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH*²⁴⁸ the CJEU was asked whether Articles 2(f) and 5(3) of the ePrivacy Directive should have been interpreted differently in case the information stored or accessed on a website user’s terminal equipment would represent personal data or not. As the ePrivacy Directive referred specifically to ‘information’, the CJEU found that the protection afforded was broader than that of Article 8 CFERU and aimed at protecting the user from interference with his or her private life. Therefore, these Articles should have been interpreted as complementary to the regulations of the DPD. In the CJEU’s words:

‘[...] any information stored in the terminal equipment of users of electronic communications networks are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms’²⁴⁹.

Another example of this is the judgment *État luxembourgeois v B, and État luxembourgeois v B, C, D, F.C*²⁵⁰ where the CJEU granted different levels of protection to the parties involved depending on whether Article 8 of the CFREU could have been applied or not. Specifically, the High Court did not guarantee the right to appeal against an order on the disclosure of information directed at the Luxembourg tax administration, neither to the taxpayer/data subject, nor to third parties affected by that order: while the former should have not conferred the right to access his/her data unless the tax investigation had issued a request of correction or adjustment, the latter could in no case benefit from the protection of Article 8, but instead would fall under Article 7 of the CFREU as secondary law excludes legal persons from its scope²⁵¹. The Court was reticent in recognising Article 7 as a direct,

²⁴⁷ Shortcomings related to the applicability of the CFREU stemming from the scope of EU law with regard to the exemption of national security were highlighted by the Working Document of the Article 29 DPWP on *surveillance of electronic communications for intelligence and national security purposes*, Brussels, 5.12.2014, p. 30. In those cases where neither Article 8 nor Article 7 can be applied, the Article 29 DPWP recalls that Member States are internationally committed with the Council of Europe. Although still valid, the Opinion should be revised in the light of the strict interpretation given by the CJEU of Article 4(2) TEU.

²⁴⁸ See the C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH*, para. 70.

²⁴⁹ *Ibidem*.

²⁵⁰ C-245/19 and C-246/19, *État luxembourgeois v B, and État luxembourgeois v B, C, D, F.C.*, 6 October 2020, EU:C:2020:795.

²⁵¹ C-245/19 and C-246/19, *État luxembourgeois v B, and État luxembourgeois v B, C, D, F.C.*, paras. 82 and 96. Angela Ward, “Article 51 – Field of Application”, in Tamara Hervej, Jeff Kenner, and Angela Ward, *op. cit.*, pp. 1413-1454, highlights that the word ‘principle’ is differently interpreted by scholars: ‘One side argues that principles may never be enforced before the courts, unless they do in reliance on EU measures or national laws implementing them, whilst the other advocates limited justiciability, confining the utility of principles to the setting aside of conflicting national legislation to stop the adoption of regressive measures’.

enforceable right but not as general principles of EU law. The Court then recalled that a breach of Article 7 demanded companies to demonstrate that they were the victims of an arbitrary or disproportionate intervention *vis-à-vis* public authorities²⁵²:

‘Therefore, such third parties must be granted the right to an effective remedy when confronted with a decision ordering that information be provided which could infringe their right to that protection’²⁵³.

From the time being, a secession of Article 8 from Article 7 CFREU has *de facto* not happened and might never occur until the former is understood as one of the multiple interpretations of the latter²⁵⁴. Therefore, and even if the EU has not acceded to the ECHR yet²⁵⁵, still the interpretation given by the ECtHR jurisprudence of Article 8 ECHR is a valuable point of reference for the Court of Luxembourg²⁵⁶. The Declaration concerning the CFREU affirms that this ‘[...] has legally binding force, confirms the fundamental rights guaranteed by the [ECHR] and as they result from the constitutional traditions common to the Member States’²⁵⁷. In addition, Articles 52(3) and 53 of the CFREU state that the rights

²⁵² C-46/87 and C-227/88, *Hoechst v Commission*, 21 September 1989, EU:C:1989:337, para. 19, and C-358/16, *UBS Europe and Others*, 13 September 2018, EU:C:2018:715, para. 56. On the application of the CFREU to private legal entities and public authorities see Manon Julicher, Marina Henriques, Aina Amat Blai, and Pasquale Policastro, “Protection of the EU Charter for Private Legal Entities and Public Authorities? The Personal Scope of Fundamental Rights within Europe Compared”, *Utrecht Law Review*, Vol. 15, No. 1, 2019, pp. 1-25.

²⁵³ C-245/19 and C-246/19, *État luxembourgeois v B, and État luxembourgeois v B, C, D, F.C.*, para. 97. See our comments in Francesca Tassinari, “La transmisión de información fiscal frente a la Carta de Derechos Fundamentales: reflexiones sobre la Sentencia del Tribunal de Justicia de 6 de octubre de 2020, *État luxembourgeois*”, *Revista de Derecho Comunitario Europeo*, No. 69, 2021, pp. 683-703.

²⁵⁴ Among others, Mariusz Krzysztofek, *GDPR: Personal Data Protection in the European Union*, The Netherlands/United States, Wolters Kluwer, p. 11 ff.

²⁵⁵ See the Protocol No 8 relating to Article 6(2) of the Treaty on European Union on the accession of the Union to the European Convention on the Protection of Human Rights and Fundamental Freedoms, *OJ C* 326, 26.10.2012, p. 273, the *Opinion 2/94*, 28 March 1996, EU:C:1996:140, the *Opinion 2/13*, 18 December 2014, EU:C:2014:2454, and, for example: Serena Forlati, “Il Parere 2/13 Della Corte Di Giustizia Dell’Unione Europea: Quale Avvenire Per Lo Spazio Di Libertà, Sicurezza e Giustizia e Per La Tutela Multilivello Dei Diritti Fondamentali In Europa?”, in VV. AA., *Globalización, Derecho y Cambios Sociales*, Santa Fe Argentina, Universidad Nacional del Litoral, 2017, pp. 205-231; Rafael Marin Aís, *La participación de la Unión Europea en tratados internacionales para la protección de los derechos humanos*, Madrid, Tecnos, 2013, and Joni Heliskowski, “The Arrangement Governing the Relationship between the ECtHR and the CJEU in the Draft Treaty on the Accession of the EU to the ECHR”, in Marise Cremona and Anne Thies, *op. cit.*, pp. 223-248.

²⁵⁶ See Article 6(3) TEU and the Declaration on Article 6(2) of the Treaty on European Union, *OJ C* 202, 7.6.2016, p. 337:

‘The Conference agrees that the Union’s accession to the European Convention for the Protection of Human Rights and Fundamental Freedoms should be arranged in such a way as to preserve the specific features of Union law. In this connection, the Conference notes the existence of a regular dialogue between the Court of Justice of the European Union and the European Court of Human Rights; such dialogue could be reinforced when the Union accedes to that Convention’.

²⁵⁷ Declaration concerning the Charter of Fundamental Rights of the European Union, *OJ C* 202, 7.6.2016, p. 337.

listed in the CFREU shall be interpreted on at least the same level as those of the ECHR²⁵⁸ and in no case should be understood as restricting or adversely affecting human rights and fundamental freedoms enshrined in the ECHR and other binding international instruments. Therefore, the Strasbourg Court's jurisprudence still informs CJEU case-law as driving principles of the EU legal order²⁵⁹, though its judgments are incorporated with a certain degree of flexibility before the recognition of a specific fundamental right protecting personal data in the EU legal order²⁶⁰. The case-law on mass surveillance developed by the CJEU in recent years shows how the recognition of a new right on the protection of personal data details and completes the ECtHR statements based on its Article 8 ECHR, namely the right to respect for private and family life²⁶¹.

In *La Quadrature du Net and Others v Premier Ministre*²⁶² the CJEU clarified whether Article 15(1) of the ePrivacy Directive precludes the implementation of a national law that, firstly, requires communication service providers to implement measures allowing the automated analysis and real-time collection of traffic and location data and, secondly, real-time collection of technical-data concerning the location of the terminal equipment used, but which makes no provision for the persons whose data is being collected and processed to be notified²⁶³. In relation to the automated analysis and real-time collection of traffic and location data, the CJEU noted that this operation consisted of the screening of data previously stored by communication service providers at the request of the relevant national

²⁵⁸ The ECtHR, for its part, evaluated the EU human right system as 'at least equivalent' to the ECHR one in its historical judgment *Bosphorus hava yollari turizm ve ticaret anonim şirketi v Ireland*, No. 45036/98, 30 June 2005, CE:ECHR:2005:0630JUD004503698.

²⁵⁹ See the Assessment of the EDPS on *the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, Brussels, 11.04.2017, p. 6, according to whom: '[...] the criteria in Article 8(2) ECHR - and specifically the condition for a limitation to be necessary in a democratic society, as interpreted in the case-law of the ECtHR, should also be taken into account in the analysis'. Also, see the Recommendation of the European Data Protection Board (EDPB) No. 02/2020 on *the European Essential Guarantees for surveillance measures*, Brussels, 10.11.2020.

²⁶⁰ Marton Varju, "European human rights law as a multi-layered human rights regime. Preserving diversity and promoting human rights", in Erik Wetzel, *The EU as a "Global Player" in Human Rights?*, Oxon, Routledge, 2011, pp. 49-65, p. 55 ff.: 'the element of flexibility is essential to maintaining the integrity of the multi-layered European Human Rights system which is riddled with intra-systemic tensions resulting from the supposed diversity of its components'. On the evolution of the tortuous relationship between the EU and the Council of Europe see Luísa Lourenço, "European Economic Area (EEA) and European Free Trade Association (ESTA)", in Ramses A. Wessel and Jed Odermatt, 2019, *op. cit.*, pp. 507-528, and Steven Greer, Janneke Gerards, and Rose Slowe, *Human Rights in the Council of Europe and the European Union. Achievements, Trends, and Challenges*, Cambridge, Cambridge Studies in European Law and Policy, 2018.

²⁶¹ The Explanations relating to the Charter of Fundamental Rights, *OJ C 303*, 14.12.2007, pp. 17-35, states that the DPD and the ECDPR '[...] contain conditions and limitations for the exercise of the right to the protection of personal data'.

²⁶² C-511/18, C-512/18 and C-520/18, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, v Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées*, 6 October 2020, EU:C:2020:791.

²⁶³ *Ibid.*, para. 169.

authorities and on the basis of the parameters established by them. Thus, the treatment of the data should be considered as generalised and undifferentiated though conducted with the help of an automated process. This operation is followed by a second step in which data on the individuals identified by the automated process is gathered accordingly. As this is serious interference with the individuals' fundamental rights enshrined by the CFREU – namely, Articles 7, 8 and 11 – that lastly enables to unknowledge which type of information is consulted online, the CJEU stressed the need for it to be compatible with the parameters set forth in Article 52(1) of the CFREU. In the light of the principle of proportionality, the CJEU emphasised that national laws should set forth substantial and procedural guarantees. Any serious interference, made on a generalised and undifferentiated basis regarding traffic and location data, especially if conducted by automated means, requires that the Member State is facing a serious threat to national security²⁶⁴ that turns out to be real, actual, or foreseeable, which can only result in time-limited storage of data²⁶⁵. Moreover, to guarantee the effectiveness of such limitations, the automated processing shall be revised by a judge or

²⁶⁴ *Ibid.*, paras. 135, including ‘the prevention and repression of activities which seriously destabilise the fundamental constitutional, political, economic or social structures of a country, and in particular directly threaten society, the population or the State as such’. In Opinion of Advocate General Sánchez Bordona, C-339/20 and C-397/20, *VD (C-339/20), SR (C-397/20)*, 18 November 2021, EU:C:2021:940: ‘[...] the sense of the judgment in *La Quadrature du Net* would not be respected if its findings on national security could be extrapolated to criminal offences, even serious ones, which affect not national security but public security or other legally protected interests. It is for this reason that the Court carefully distinguished between national legislative measures which provide for the general and indiscriminate retention of traffic and location data for the purposes of protecting national security [...] and those which concern the combating of crime and the safeguarding of public security [...]. Those two types of measure cannot have the same scope, as that distinction would otherwise be rendered meaningless’ (paras. 78-79). Specifically, the Advocate General found that the records/recordings held by a telecommunications operator according to Article 12(2)(d) of Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation (market abuse), *OJ L 96*, 12.4.2003, pp. 16-25, and Article 23(2)(g) and (h) of Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC Text with EEA relevance, *OJ L 173*, 12.6.2014, pp. 1-61, must be interpreted as to be retained for the purposes of combating serious crime and safeguarding public security, but not for the purposes of safeguarding national security.

²⁶⁵ *Ibid.*, para. 146, and the Opinion of Advocate General Sánchez Bordona, C-793/19 and C-794/19, *Bundesrepublik Deutschland v SpaceNet AG (C-793/19) Telekom Deutschland GmbH (C-794/19)*, 18 November 2021, EU:C:2021:939, para. 84. In C-207/16, *Ministerio Fiscal*, 2 October 2018, EU:C:2018:788, para. 57, the CJEU maintained that ePrivacy Directive also enables a general interference justified on the basis of the prevention, investigation, detection, and prosecution of not-serious criminal offences. Yet, it shall be outlined that in *Ministerio Fiscal* the CJEU was evaluating the access to personal data in the frame of a criminal proceeding provided of appropriate safeguards conferred by the judicial authority, and not concerning ‘freelance’ law enforcement or intelligence services activities as it did in C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, para. 97. Here the CJEU noted that only the fight against serious crime could have justified a serious interference in individuals’ private lives. On the notion of “serious crime” see Stefania Carnevale, Serena Forlati, and Orsetta Giolo, *Redefining Organised Crime: A Challenge for the European Union?*, Oxford, Hart Publishing, 2017, and Lucas J. Ruiz Díaz, *La acción exterior de la Unión Europea contra el Crimen Organizado Transnacional: Aspectos internos y dinámicas externas del discurso securitario*, Madrid, Tecnos, 2017.

independent administrative authority with binding effects aiming at verifying the existence of such threatening circumstances and the respect of the guarantees established by law.

Nevertheless, the CJEU prohibited the possibility that automated filtering could be based on sensitive data²⁶⁶ and finally added that any positive outcome (or match) stemming from the automated processing, should be revised by an individual, and that the reliability and updating of such models and pre-established criteria should be monitored through regular testing. As for the real-time collection of technical data concerning the location of the terminal equipment used, the CJEU affirmed that this processing could be only conducted with regard to a person previously identified as potentially linked to a terrorist threat²⁶⁷. It specified that this measure enables ‘[...] national competent authorities to monitor, for the duration of the authorisation, continuously and in real time, the persons with whom those persons are communicating, the means that they use, the duration of their communications and their places of residence and movements. It may also reveal the type of information consulted online’²⁶⁸. The collection of real-time data related to the gathering of traffic data and the location of terminal equipment were directly passed to the French Prime Minister. Such a serious degree of interference should be evaluated differently than the one stemming from non-real time access: only persons for whom there is a valid reason to suspect involvement, to some degree, in terrorist activities can be subjected to such measures. Furthermore, the law allowing the real-time collection of data should be founded on objective criteria established by national legislation, including the circumstances and conditions under which such processing can be authorised. All in all, the CJEU recalled that an *ex ante* control by a judicial or an independent administrative body should verify that the order is limited to what is strictly necessary.

As far as the right to information for persons whose data had been gathered or analysed was concerned, the CJEU decided that in the framework of an automated analysis of traffic and location data, national authorities shall publish general information with regard to the analysis, without being obliged to inform individuals on a case by case basis; yet, in cases where an individual is identified following the automated filtering, then, the individual has the right to be informed in order to exercise his/her data protection rights, unless such notification undermines the authorities’ functions²⁶⁹.

²⁶⁶ *Ibid.*, para. 181.

²⁶⁷ *Ibid.*, para. 183.

²⁶⁸ *Ibid.*, para. 184.

²⁶⁹ *Ibid.*, para. 191. The CJEU then passed to interpret the depositions of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *OJ L 178*,

La Quadrature du Net was resolved a few months before *Big Brother Watch and Others v The United Kingdom* and we believe that it was decisive in encouraging the Strasbourg Court to embark on a new round of case law regarding mass surveillance. The EU accession to Convention 108+ – during the creation of which the EU played a prominent role – and potentially to the ECHR, are expected to bring the two Courts closer together. However, the CJEU might maintain a certain level of autonomy from Strasbourg on the basis of specific Articles within the CFREU, the implementation of EU law to which its interpretative function is limited to, and an own data governance strategy for the digital decade²⁷⁰. From these statements the EU strategy becomes understandable: it wants not only to contribute to the international dialogue on the protection of personal data²⁷¹, but also aims at occupying a leading role by exporting the EU data management model worldwide²⁷².

17.7.2000, pp. 1-16 (eCommerce Directive), in light of Articles 6, 8, 11, 52(1) of the CFREU. The referral judge asked whether a national legislation conferring providers of access to online public communication services and hosting service providers to retain, generally and indiscriminately, *inter alia*, personal data relating to those services, is lawful or not. The CJEU found that information society services – such as services providing access to the Internet or to a communication network and hosting services – contemplated in Article 2(a) of eCommerce Directive should be considered as electronic communication services regulated under the ePrivacy Directive. Hence, the access to online public communication services and hosting service providers retaining personal data related to those services, generally and indiscriminately, should be considered to be contrary to the EU data protection *acquis* in the light of with Articles 7, 8, 11, and 52(1) of the CFREU.

²⁷⁰ “Droits et principes numériques, la Présidence française du Conseil de l'UE met l'accent sur le respect des droits de l'Homme”, *Bulletin Quotidien Europe*, No. 12942, 30.4.2022.

²⁷¹ See the “La Commission européenne rappelle que la protection des données n'est pas un luxe, mais une nécessité”, *Bulletin Quotidien Europe*, No. 12412, 28.1.2020: ‘Twenty months after the entry into force of the General Data Protection Regulation (GDPR), the European Commission is pleased that the regulation has acted as a catalyst to put data protection at the center of many ongoing, but also future, policy debates with the development of 5G and artificial intelligence’ – our own translation. Less strong seems to be the EU as a global standards settler in the field of AI, especially with regard to the US – see the “Intelligence artificielle et stratégie de données, les eurodéputés se penchent sur le sujet de la coopération internationale”, *Bulletin Quotidien Europe*, No. 12802, 1.10.2021, and Jana Puglierin, “Priorities for the EU's New Foreign Policy Agenda up to 2024: Unleashing the Potential of the Common Foreign and Security Policy”, *DGAP Analysis*, No. 1, 2019, p. 12.

²⁷² According to Luxembourg Prime Minister Xavier Bettel ‘It is important to do everything possible today to make Europe a world leader. Transformation is a high-speed train, we cannot afford to stay on the platform’, in “Commissioner Thierry Breton inaugurates the headquarters of the European Joint Undertaking for High Performance Computing in Luxembourg”, *Bulletin Quotidien Europe*, No. 12711, 4.5.2021 (our own translation).

3. European Union's competence on the protection of personal data and on the free movement of such data

Under the Lisbon Treaty, Article 286 of the 1997 TEC was “replaced”²⁷³ by Article 16 TFEU²⁷⁴ and the following instruments were duly taken into account: the DPD; Article 8 of the ECHR; the Convention 108, and the ECDPR²⁷⁵. Article 16 TFEU confers upon the EU an express internal competence regarding the protection of personal data and on the free movement of such data. According to Article 16 TFEU:

‘1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices, and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data.

3. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union’.

The following sections will analyse the nature and characteristics of this new competence, namely its shared exercise and sectorial application in the AFSJ.

3.1. Article 16 of the Treaty on the Functioning of the European Union as a shared competence: Justifying subsidiarity, necessity, and proportionality in the light of the European Union's Charter of Fundamental Rights

Despite not being listed in the EU competence catalogue²⁷⁶, Article 16 TFEU empowers the EU to adopt measures to protect personal data and to guarantee the free movement of such data which shall be regarded as a shared competence between the EU and its Member

²⁷³ In reality, the scope of Article 16 TFEU is bigger than previous Article 286 of the 1997 TEC and its insertion was expected to support the adoption of “specific juridical acts” – see José Martín y Pérez de Nanclares, “Artículo 8: Protección de datos de carácter personal”, in Araceli Mangas Martín, *Carta de Derechos Fundamentales de la Unión Europea: Comentario Artículo por Artículo*, Madrid, Fundación BBVA, 2008, pp. 223-243, p. 228.

²⁷⁴ The provision of a new Article had already been debated on the occasion of the (failed) project on a Constitution for Europe. See, for example, the Council of the EU, 2003 IGC – *Draft Treaty establishing a Constitution for Europe (following editorial and legal adjustments by the Working Party of IGC Legal Experts)* I, CIG 50/03, Brussels, 25 November 2003 (26.11), p. 56.

²⁷⁵ See the Council of the EU, *IGC 2007 Draft declarations*, CIG 3/07, Brussels, 23 July 2007 (26.07), p. 27.

²⁷⁶ Articles 3, 4, and 6 TFEU.

States²⁷⁷. Through the conferral²⁷⁸ of shared competences, Member States empowered the EU to act in a specific domain and to achieve a specific objective so that their national freedom to act exists up until the point that the EU adopts its own rules – this is known as pre-emption principle²⁷⁹. “Old pre-emption”²⁸⁰ implies that once the EU acts, it assumes exclusive competence in the field that it has occupied and to the extent to which it has occupied it until Member States restore their exercise when or if the EU abandons it²⁸¹. The exercise of shared competences is regulated by the principles of subsidiarity, necessity, and proportionality as Bradley summarises:

‘Conferral determines what competences the Union enjoys, subsidiarity provides a test as to whether or not they should be exercised in a given case, and proportionality seeks to ensure the competences are exercised in such a manner as to encroach on the competences of the Member States, and the rights of individuals, as little as possible’²⁸².

Any legislative proposal presented by the European Commission must comply with these principles, first of all, by consulting national Parliaments in respect of the subsidiarity principle and through its impact assessment document, which includes evaluation of the proposal’s financial impact, as well as the qualitative and quantitative indicators that show that the objective is better pursued at the EU level²⁸³. Once the necessity of a supranational intervention is justified, then, the principle of proportionality regulates the intensity with which the EU should legislate.

In the case of Article 16 TFEU, these principles assume different connotations than those mentioned above, as the fundamental rights approach appears to displace the competential one. As Prof. Muir highlights:

²⁷⁷ See Article 4(1) of the TFEU: ‘The Union shall share competence with the Member States where the Treaties confer on it a competence which does not relate to the areas referred to in Articles 3 and 6’.

²⁷⁸ Article 5(2) TEU: ‘Under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States’.

²⁷⁹ Stephen Weatherill, “Beyond Preemption? Shared Competences and Constitutional Change in the European Community”, in David O’ Keefe and Patrick M Twomey, *Legal Issues of the Maastricht Treaty*, London/New York, Chancery Law Publishing, 1994, pp. 227-230. The author points out that regulations aside, being these directly applicable and prevailing on national law for, ‘[...] the Court’s ruling that even wrongfully unimplemented Directives may achieve the preemptive effect, directly or perhaps even, albeit less satisfactory, indirectly, despite the limitations on the reach of Directives into the national legal order suggested by Article 189’s reference to implementation according to national choice of form and methods’, p. 17.

²⁸⁰ *Ibid.*, p. 28.

²⁸¹ See Article 5(2) TEU.

²⁸² See Kieran St C Bradley, “Legislation in the European Union”, in Catherine Barnard and Steve Peers, *European Union Law*, Oxford, Oxford University Press, 2017, pp. 97-142, p. 105. The author underlines that the Single European Act and the Maastricht Treaty firstly opted for the use of the word ‘competence’ inspire of ‘powers’ precisely when the European Community expanded significantly its ‘formal powers’ later on bridled by the Lisbon Treaty.

²⁸³ See Protocol No 2 on the application of the principles of subsidiarity and proportionality, *OJ* 115, 09.05.2008, pp. 206-209.

‘There is thus an inherent tension between the doctrine of allocation of competences and the dynamics of fundamental rights protection. While the doctrine of allocation of competences is thought to be the umbilical cord feeding the existence and growth of EU competences, fundamental rights protection constantly questions this one-sided feeding process in the context of both the EU passive and active protection systems. The logic of fundamental rights protection relies on a universalized and supreme vision of mankind that is designed and destined to test the limits of public control. An ever-stronger fundamental rights discourse at EU level is thus hard to reconcile with the traditional doctrine of attributed competences seeking to circumscribe EU constraints on domestic policies’²⁸⁴.

In other words, while the exercise of sovereign competences is by definition “particular”, and is limited to a specific territory and jurisdiction – or competence, in the case of the EU –, the respect and protection of human rights – in the specific case of the EU, of fundamental rights – apparently knows no limits. This rationale explains why Article 16 TFEU has been strategically inserted within the provisions of the founding Treaty having general application: Article 16 TFEU’s cross-cutting dimension confirms that the right to the protection of personal data must be respected (and protected) in the framework of every policy within the Union²⁸⁵.

However, the founding Treaties do not confer to the EU general competences on fundamental rights. The CFREU leaves clear that its scope of application is limited to the EU’s institutions, bodies, offices, and agencies, as well as to the Member States, while implementing of EU law²⁸⁶ which ‘[...] seems to reflect a general understanding that EU fundamental rights obligations simply track EU activities, whether they take place within or without territorial boundaries’²⁸⁷. Though the CFREU is one of several sources²⁸⁸ integrating

²⁸⁴ Elise Muir, “Fundamental Rights: An Unsettling EU Competence”, *Human Rights Review*, 2014, Vol. 15, pp. 25-37, p. 35.

²⁸⁵ C-617/10, *Åklagaren v Hans Åkerberg Fransson*, 26 February 2013, EU:C:2013:105. Article 51(1) of the CFREU: ‘The provisions of this Charter are addressed to the institutions, bodies, offices and agencies of the Union [...] They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties’. Articles 2(1) and 3(5) TFEU set forth the EU commitment in respecting and protecting human rights respectively. However, the latter really refers to the EU ‘relations with the wider world’ only.

²⁸⁶ Article 51(1) of the CFREU: ‘The provisions of this Charter are addressed to the institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law’.

²⁸⁷ Violeta Moreno-Lax and Cathryn Costello, “The Extraterritorial Application of the EU Charter of Fundamental Rights: From Territoriality to Facticity, the Effectiveness Model”, in Steve Peers, Tamara Hervey, Jeff Kenner, and Angela Ward, *op. cit.*, pp. 167-1583, para. 9.10.

²⁸⁸ See Article 6(3) TEU and Paul De Hert, “EU criminal law and fundamental rights”, in Valsamis Mitsilegas, Maria Bergström, Theodore Konstadinides, *Research Handbook on EU Criminal Law*, Cheltenham, Elgar Edward Publishing, 2016, pp. 105-124, p. 108. The other two sources are general principles of fundamental rights, as recognised by the Member States’ constitutional traditions – that is general principles of domestic law according to Articles 6(1) and 51(1) CFREU – and binding international instruments to which Member States and/or the EU adhere to – by virtue of Article 6(3) TEU.

the multi-layered regime on the protection of human rights within the EU²⁸⁹, it ‘does not extend the field of application of Union law beyond the powers of the Union or establish any new power or task for the Union, or modify powers and tasks as defined by the Treaties’²⁹⁰. Therefore, we believe that the principle of conferral on the one hand, and the principle of subsidiarity and proportionality on the other, must be interpreted in regard to the CFREU, which does not necessarily conflict with the competence reading usually made along these principles. In the following paragraphs, we will analyse how the principles of subsidiarity and proportionality are shaped with regard to the CFERU when the EU exercises its competence on the protection of personal data.

3.1.1. The principle of subsidiarity

In order to balance central and national synergies, the principle of subsidiarity has been integrated²⁹¹ in the EU legal order following the example of federal constitutional systems²⁹². According to this principle, the EU action shall be undertaken when the objectives pursued by the EU cannot be sufficiently achieved by the Member States, either at a central or regional level, but can be better achieved at the Union level, by reason of the scale or effects of the proposed action²⁹³. National Parliaments can intervene in the legislative procedures to monitor its respect²⁹⁴ and may even reject a draft legislative act in cases of non-compliance

²⁸⁹ Marton Varju, *op. cit.*, p. 50, describes their interactions as ‘flexibly inter-connected system of human rights regimes where intra-systemic communication is performed in the hierarchical orders among the participating regimes’.

²⁹⁰ See the Declaration concerning the Charter of Fundamental Rights of the European Union, *OJ C* 202, 7.6.2016, p. 337, and Article 6(1), second paragraph, of the TEU.

²⁹¹ See Article 3b of the TEEC, Article 25 of the Single European Act, *OJ L* 169, 29.6.1987, pp. 1-28, and in the 1992 TEU, Article A and B of Title I, as well as Article K.3(2)(b) of Title VI. At that time, the EU was not provided with a competence catalogue that marked the guidelines on the nature of the EU competence and the scope of the subsidiarity principle was not clear before the lack of a systematisation of EU competences. A. G. Toth, “Legal Analysis of subsidiarity”, in David O’ Keefe and Patrick M. Twomey, *op. cit.*, 1994, pp. 37-48, underlines that the existence of interlink features between different EU policies, one exclusive and the other one shared, may have scarified the principle of subsidiarity whether the former would have prevailed on the latter.

²⁹² See, for example: Koen Lenaerts, “Constitutionalism and the Many Faces of Federalism”, *The American Journal of Comparative Law*, No. 38, 1990, pp. 205-263; Koen Lenaerts and Jean-Pascal Van Ypersele, “Le principe de subsidiarité et son contexte”, *Cahiers de Droit Européen*, No. 30, 1994, pp. 3-85; Vlad Constantinesco, “Who’s afraid of Subsidiarity?”, *Yearbook of European Law*, Vol. 1, No. 1, 1991, pp. 33-55; Katarzyna Granat, *The principle of subsidiarity and Its enforcement in the EU Legal Order: The Role of National Parliaments in the Early Warning System*, Oxford, Hart Publishing, 2018.

²⁹³ A. G. Toth, *loc. cit.*, underlines that these two testes, although generally aligned, may flow into different outcomes in case the effectiveness test requires the EU action while the scale test justified the national intervention, or vice versa.

²⁹⁴ See Article 5(3) TEU *in fine* recalling the Protocol No 2. A first Protocol on the application of the principles of subsidiarity and proportionality, *OJ C* 340, 10.11.1997, p. 105, was attached to the Amsterdam Treaty. The European Commission provides to the Council and the Parliament an annual report on subsidiarity, proportionality and the relation between the EU Institutions and the national Parliaments. The reports are all available in the European Commission’s official webpage, www.europa.eu.

with the subsidiarity principle²⁹⁵. In reality, subsidiarity has been found to have a dynamic nature that enables both the expansion and restriction of EU intervention in the light of the treaties' objectives²⁹⁶. In Prof. Steiner's words:

‘The concept of cross border or spillover effect may itself be constructed strictly, as meaning that the problem in question, because of its dimension, cannot be dealt with effectively at national level, or broadly, as meaning that regulation at national level is undesirable because of its repercussion, on the single market’²⁹⁷.

All in all, the principle of subsidiarity can be used both to promote and to limit centralisation according to the political approaches agreed upon by the co-legislators²⁹⁸. In this sense, subsidiarity can be easily justified under internal market logic, which aims at eliminating barriers to the free movement of goods, persons, services, and capital, and to prevent the existence of less rigorous standards in some Member States from undermining competition within the EU²⁹⁹.

This logic is not far removed from that exhibited by European Community in the early days of its data protection legislative framework: The creation of the DPD was justified on the basis of an urgent need for an approximation of the Member States' legal orders so as to promote the smooth flow of data on the assumption that the Member States' unilateral,

²⁹⁵ The ‘yellow card’ imposes to the European Parliament, the Council, and the European Commission, and, where appropriate, a group of Member States, the CJEU, the European Central Bank or the European Investment Bank to revise the legislative proposal in case one third of the votes allocated to the national Parliaments points out that the draft measure does not comply with the principle of subsidiarity – see Article 7 of Protocol No 2. This threshold is lowered to a quarter in case of legislative acts based on Article 76 TFEU, namely all the measures adopted under Chapters 4 and 5 of Title V TFEU, as well as Article 74 TFEU on the administrative cooperation among the Member States and among the Member States and the European Union – see Article 7(2) of Protocol No 2. The ‘orange card’, instead, is triggered by the simple majority of the votes allocated to national Parliaments and differentiates from the former because in case the European Commission decides to maintain the proposal, not only it is required to justify it, but it shall also submit the proposal to the co-legislators for its revision – see Article 7(3) of Protocol No 2. A 55% majority of the members of the Council or a majority of the votes cast in the European Parliament can turn down the legislative proposal in case it is considered to breach the subsidiarity principle.

²⁹⁶ See the Conclusions of the Presidency of the European Council, Edinburgh, 11-12 December 1992.

²⁹⁷ Josephine Steiner, “Subsidiarity under the Maastricht Treaty”, in David O’ Keefe and Patrick M. Twomey, *op. cit.*, pp. 49-64, p. 50. A critic is made also by Stephen Weatherill, *loc. cit.*

²⁹⁸ Paolo G. Carozza: “Subsidiarity as a Structural Principle of International Human Rights Law”, *American Journal of International Law*, Vol. 97, No. 1, 2003, pp. 38-79, p. 44:

‘Subsidiarity is therefore a somewhat paradoxical principle. It limits the state, yet empowers and justifies it. It limits intervention, yet requires it. It expresses both a positive and a negative vision of the role of the state with respect to society and the individual. That duality appeared in the first variations of the principle articulated by Leo XIII and Pius XI, and is still evident in much of the disagreement about the proper application of the principle today [...]’.

²⁹⁹ Jacques Delors, *Subsidiarity: The Challenge of Change. Proceedings of the Jacques Delors Colloquium*, Maastricht, European Institute of Public Administration, 1991, and José Martín y Pérez de Nanclares, 1997, *op. cit.*, pp. 114-115 (our own translation):

‘Subsidiarity in the TEC can only be interpreted as a principle of a functional and bottom-up nature aimed at supporting the supranational (federal) level in matters in which, because Community intervention is necessary and more effective, the lower level (the Member States) has renounced the exercise of certain competences which were initially the sovereign competence of that lower level’.

bilateral, or multilateral actions would have jeopardised the internal market project. In the proposal, the European Commission pointed out that the Directive should have constituted the ‘centerpiece of the protection system’³⁰⁰. Despite controversies³⁰¹, we agree with the European Commission’s position, that justified the European Community’s intervention by reason of the scale or effects of the proposed action only in respect of the one of the two sides of the Union’s competence on personal data. In support of this intervention, we recall that the DPD was a pioneer in setting down rules not only on the protection of personal data, but also on its transborder flow among the Member States³⁰² and its transfer to third countries³⁰³. The latter, in particular, was a necessary tool for the expansion of international trade³⁰⁴ and was regulated as a data processing activity³⁰⁵ the lawfulness of which should have been assessed on the basis of the specific provisions set forth by the organisation³⁰⁶. If the EU had not intervened, data protection issues would have remained anchored to national and international frameworks regulating the right to privacy without paying attention to the challenges new (digital) technologies were posing. In addition, the DPD rules on the transfer of personal data pre-dated those of the Council of Europe, which took them as a point of reference in the First Additional Protocol of 2001 to Convention 108. Provided that the transposition of Convention 108 into the Member States’ legal orders would be (if it took place) a long and cumbersome process, the EU’s intervention determined a point of no return, especially for those Member States that were the most hostile to the regulation of the processing of personal data. Where international law had failed to settle differences between states, supranational law had succeeded in imposing itself.

³⁰⁰ *Ibid.*, p. 6.

³⁰¹ Carlos Ruiz Miguel, *op. cit.*

³⁰² Article 1(2) of the DPD: ‘Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1’. Article 12(2) of the Convention 108, instead, established that the contracting parties should have not refrained the flow of data for reasons of privacy concerns only, but its third paragraph allowed them for derogating it when: the legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other party provide an equivalent protection, or the transfer is made from its territory to the territory of a non-contracting state through the intermediary of the territory of another party, in order to avoid such transfers resulting in circumvention of the legislation of the party.

³⁰³ Chapter IV of the DPD.

³⁰⁴ Recital (56) DPD:

‘Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations’.

³⁰⁵ C-317/04 and C-318/04, *Parliament v Council of the European Union and Commission of the European Communities*, para. 56.

³⁰⁶ C-101/01, *Bodil Lindqvist v Åklagarkammaren i Jönköping*.

Recalling Article 8 of the CFREU³⁰⁷ led some scholars to believe that the incorporation of Article 16 into the TFEU shifted the centre of gravity of the EU policy on personal data from the promotion of its free movement to the protection of individuals' fundamental rights³⁰⁸. Notwithstanding the fact that the Treaty of Lisbon clearly strengthens the fundamental rights approach by upgrading the legal value of the CFREU to primary law, we believe that the EU competence on the protection of personal data enshrined in Article 16 TFEU is always underpinned by a twofold purpose, at least as far as its internal application is concerned. According to Hijmans:

‘[t]his obviously does not mean that two different sets of rules are needed, but it would mean that not all the rules adopted under Article 16(2) aim at respecting an individual's right to data protection; they could also relate to the free movement of data. This latter option would mean that the GDPR could include rules that facilitate the free movement of data, but not necessarily deliver data protection. Possibly, some of the Provisions of Chapter V GDPR on the transfer of personal data could be read in this perspective’³⁰⁹.

Similarly, Prof. Lynskey maintains that the free flow of personal data is no longer the predominant perspective, and the two objectives are now equally relevant³¹⁰. The objectives are complementary to one another since the regulation on the sharing of personal data does not set aside the protective approach³¹¹. Indeed, any processing activity, including the exchange of data among Member States, constitutes an interference with the fundamental right to the protection of personal data³¹². However, although data protection and the free movement of data are dealt with together by the co-legislators, one of the two sides can prevail over the other one. Specifically, Article 16(2) TFEU allows the EU to adopt measures to protect individuals' fundamental rights as well as legislative reforms to regulate the

³⁰⁷ Article 16(1) TFEU: ‘Everyone has the right to the protection of personal data concerning them’.

³⁰⁸ See Hielke Hijmans, 2016, *op. cit.*, p. 51. According to the author: ‘In the Court's case law, fundamental rights have become more important and the Charter has become the yardstick for a strict scrutiny of acts of the EU and the Member States within the scope of EU Law’. Also, see the author in “Article 51: Supervisory Authority”, in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 863-872, p. 868.

³⁰⁹ See Hielke Hijmans, “Article 1: Subject-matter and objectives”, in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *op. cit.*, 48-59, p. 56.

³¹⁰ See Orla Lynskey, 2015, *op. cit.*, p. 62 ff.

³¹¹ José Antonio Castillo Parrilla, “The Legal Regulation of Digital Wealth: Commerce, Ownership and Inheritance of Data”, *European Review of Private Law*, No. 5, 2021, pp. 807-830, proposes to re-evaluate personal data as a “legal good” to counter-balance the fundamental right approach with the need for data to flow in a digital economy.

³¹² In this sense, see Gloria González Fuster, “Curtailling a right in flux: restrictions of the right to personal data protection”, in Artemi Rallo Lombarte and Rosario García Mahamut, *Towards a new European Data Protection Regime*, Valencia, Tirant lo Blanch, 2015, pp. 527-528. Conversely, Hielke Hijmans, 2016, *op. cit.*, at p. 60, maintains that “[...] data protection must be seen as ‘rules of the game’ or ‘a system of checks and balances’, which finds its basis in the wording of Article 8(2) Charter, as well as Directive 95/46 and other EU instruments for data protection’.

exchange of personal data among Member States³¹³. The European Commission communication on Safeguarding Privacy in a Connected World advanced a new data protection package on 25 January 2012³¹⁴ in which the DPD was substituted for the GDPR³¹⁵. The European Commission emphasised that in the 21st century, the aggregation and analysis of data constitute a new form of economic activity exploited by big private companies: ‘[...] rapid pace of technological change and globalisation have profoundly transformed the way in which an ever-increasing volume of personal data is collected, accessed, used and transferred’³¹⁶. Although the rhetoric on the free flow of data for market purposes continues through the GDPR³¹⁷, this instrument also pays great attention to the fundamental rights of the EU competence on personal data³¹⁸. Therefore, at least as far as the protective side of the EU competence based on Article 16 TFEU is concerned, the principle of subsidiarity should be re-interpreted in the light of the CFREU.

On closer inspection, a linkage between Article 16(1) TFEU and Article 8 of the CFREU was indispensable if the CFREU could in no way extend the EU catalogue of competences³¹⁹. This reminder, read in the light of the principle of subsidiarity, is noticeable. Hijmans and Scirocco find that:

‘As a consequence of the above Article 16 (1), and more in general, the right to data protection will have a similar constitutional dimension. One can even argue that all

³¹³ Hielke Hijmans, 2016, *op. cit.*, pp. 125-183, highlights that the EU competence on the protection of personal data and its free movement shall be identified in Article 16(2) TFEU that empowers to the EU legislator to adopt rules on this domain, though the organisation of independent authorities remains a national competence.

³¹⁴ See the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2012) 9 final, Brussels, 25.1.2012.

³¹⁵ The definition of processing agreed under the GDPR, Article 4(2), includes the ‘[...] collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction’ which strengthens the idea that also the flow of personal data within the EU is not a hundred percent free since in no case it can undermine a certain level of protection.

³¹⁶ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2012) 9 final, Brussels, 25.1.2012, para. 1.

³¹⁷ For example, recital (9) of the GDPR states that:

‘Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law’.

³¹⁸ Recital (1) of the GDPR: ‘The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the ‘Charter’) and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her’.

³¹⁹ Article 6(1) TEU and Article 51(2) CFREU that clearly prohibit any extension of the EU competential catalogue as a consequence of the binding force acquired by the CFREU. See also the Declaration concerning the Charter of Fundamental Rights of the European Union, *OJ C* 202, 7.6.2016, p. 337–337, whose second paragraph states: ‘The Charter does not extend the field of application of Union law beyond the powers of the Union or establish any new power or task for the Union, or modify powers and tasks as defined by the Treaties’.

persons would have a right to data protection, even in the absence of rules specifying the right, and those persons can invoke the right before a court³²⁰.

While speculating that the inclusion of the right to the protection of personal data within the Treaty's provisions may have conferred it direct application in the Member States' legal orders³²¹, Hijmans and Scirocco point out that neither Article 16 TFEU nor Article 8 of the CFREU seem to be formulated in such a way to enable individuals to pursue their rights. However, such a linkage must not be underestimated: read in conjunction with Article 8 of the CFREU, the first paragraph of Article 16 TFEU embraces logic of fundamental rights which holds that Member States are expected to firstly safeguard their citizens' rights. While the EU is better positioned to regulate cross-border phenomena³²², the Member States could make use of their constitutional prerogatives to legitimise their intervention³²³. At least this is the position that states take in international human rights law where the principle of subsidiarity is gaining increasing attention³²⁴. In this domain, subsidiarity keeps its twofold functionality as follows³²⁵: procedurally, it imposes on the individual the exhaustion of domestic remedies before they attend an international court; substantially, it respects the margin of manoeuvre left to the states, especially in cases where restrictions on human rights are permitted, while calling on the states to secure an effective protection of individuals' rights in light of the logic of "positive obligations"³²⁶.

Balancing commonality and particularity, the principle of subsidiarity has been incorporated in the CFREU³²⁷ 'as a rhetorical mediator between the universal and the

³²⁰ Hielke Hijmans and Alfonso Scirocco, *op. cit.*, p. 1518.

³²¹ The approximation of legal orders, together with the promotion of the respect of fundamental rights as a general principle of the EU legal order and a shared value among the Member States, legitimises the EU to direct its action toward the citizens themselves, instead of the Member States' governments. As Geert De Baere, "Subsidiarity as a Structural Principle Governing the use of EU External Competences", in Marise Cremona, *Structural Principles in EU External Relations Law*, Portland, Hart Publishing, 2018, pp. 71-92, highlights, the Preamble to the TEU commits the EU 'to continue the process of creating an ever closer union among the peoples of Europe, in which decisions are taken as closely as possible to the citizen in accordance with the principle of subsidiarity'.

³²² Hielke Hijmans, 2016, *op. cit.*, p. 269.

³²³ *Ibid.*, p. 153, calls it a "paradox" since although the EU is better placed to ensure privacy and data protection, Article 16 TFEU triggers the regulation of politically sensible domains that require further democratic accountability.

³²⁴ Protocol No 15 amending the Convention on the Protection of Human Rights and Fundamental Freedoms, ETS 213, signed in Brussels on 24 June 2013, entered into force on 1 August 2021. See: Alastair Mowbray, "Subsidiarity and the European Convention on Human Rights", *Human Rights Law Review*, Vol. 15, No. 2, 2015, pp. 313-341, and Robert Spano, "Universality or Diversity of Human Rights? Strasbourg in the Age of Subsidiarity", *Human Rights Law Review*, Vol. 14, No. 3, 2014, pp. 487-502.

³²⁵ Paolo G. Carozza, *op. cit.*, p. 48.

³²⁶ See *supra*.

³²⁷ See the Preamble and Article 51(1) of the CFREU. According to the latter: 'The provisions of this Charter are addressed to the institutions and bodies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law'.

particular, integration and differentiation, harmonization and diversity'³²⁸. Although the principle of subsidiarity is not usually invoked in this sense³²⁹, neither in Brussels nor in Luxembourg, we believe that this is how the linkage between Article 16(1) TFEU and Article 8 CFREU has to be read. The CJEU³³⁰ complies with the principle of subsidiarity, for example, each time it refrains from interpreting the Member States' laws when implementing the EU data protection *acquis* while referring the resolution of the case at issue to the correspondent national courts³³¹. In this case, the CJEU respects the discretion of the Member States in restricting the right consecrated under Article 8 CFREU, within the limits set out in Article 52(1) of the CFREU³³². Also, the EU contributes to the "positive" facet of subsidiarity by supporting the respect, protection, and fulfilment of the individuals' right to the protection of personal data while monitoring the compliance with the supranational obligations assumed by its Member States, that is: it does not replace the Member States' obligation to protect and ensure the rights and freedoms sealed in the CFREU, but "contributes" to their protection³³³. In sum, the right to the protection of personal data cannot be said to be "better ensured" at the EU level when compared to the national one, which rectifies our position with regard to the regulation of data flows, *ad intra* and *ad extra*, advanced above. As Prof. Carozza recalls:

‘A subsidiarity-oriented understanding of human rights and international law does not care to ask whether "state sovereignty" must either resist or give way to international harmonization and intervention but, instead, whether the good that human rights aim at realizing can be accomplished at the local level, and if not, what assistance is necessary from a more comprehensive association to enable the smaller unit to realize its role’³³⁴.

³²⁸ Paolo G. Carozza, *op. cit.*, p. 54.

³²⁹ Paul De Hert, "EU Sanctioning Powers and Data Protection: New Tools for Ensuring the Effectiveness of the GDPR in the Spirit of Cooperative Federalism", in Stefano Montaldo, Francesco Costamagna, and Alberto Miglio, *EU Law Enforcement: The Evolution of Sanctioning Powers*, Oxford, Routledge, 2021, pp. 291-324, p. 297: '[...] Article 16 TFEU intentionally draws the attention away from the normal subsidiarity principles exercise ('powers are in hands of the Member States, unless the Union can do better') and draws the data protection policy agenda to the Brussels levels, based on an implicit understanding that this area is supra national'³²⁹.

³³⁰ Gráinne de Búrca, "After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?", *Maastricht Journal of European and Comparative Law*, Vol. 20, No. 2, 2013, pp. 168-184.

³³¹ Among others, see C-136/17, *GC, AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL)*, 24 September 2019, EU:C:2019:773, para. 68.

³³² 'Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'.

³³³ Article 3(5) TEU.

³³⁴ Paolo G. Carozza, *op. cit.*, p. 66.

3.1.2. The principles of necessity and proportionality

The principles of necessity and proportionality require the intervention of the EU to be necessary and limited to the minimum required in view of the objective proposed³³⁵. In general terms, the necessity of the EU's intervention can be justified if the supranational action generates benefits when addressing a transnational problem, or if a lack of intervention of the EU might cause a distortion of the internal market³³⁶. Specifically, cross-border activities justify EU intervention when '[...] either action by supranational institutions would produce benefits or action by the Member States separately would produce costs'³³⁷. In practice, the principle of proportionality mitigates the intensity of the EU action, in terms of content and form, once it has been assessed that its intervention is needed by virtue of the principle of subsidiarity.

The distinction between the necessity of any EU intervention and its proportionality is not clearly established in the Treaties, nor has the CJEU given a consistent interpretation of the relationship between the two. Under the principle of proportionality, the CJEU evaluates: the assessment of whether the measure can achieve a legitimate aim; the necessity of the measure in terms of the possibility to envisage a less restrictive means capable of producing the same result and, finally, the evidence that the measure has not had an excessively detrimental effect on the applicant's interest. As Prof. Tridimas underlines, this tripartite test is not systematically analysed by the CJEU so that '[t]he essential feature of the principle is that the Court performs a balancing exercise between the objective perused by the measure in issue and its adverse on individual freedoms'³³⁸. This balance is generally referred to by the CJEU as 'strict necessity'³³⁹. For example, in *Volker und Markus Schecke GbR, Hartmut*

³³⁵ Article 5(4) TEU: 'Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties'.

³³⁶ See the Protocol on the application of the principles of subsidiarity and proportionality, *OJ C* 340, 10.11.1997, pp. 105.

³³⁷ See Federico Fabbrini, "The principle of subsidiarity", in Robert Schütze and Takis Tridimas, *op. cit.*, pp. 221-242, p. 226.

³³⁸ Therefore, these three elements are subject to a different degree of scrutiny by the Court which allows it to adopt different interpretation and finally promote the integration of EU policies. For example, in the evaluation of an EU policy linked to the four main EU freedoms, Takis Tridimas underlines that the CJEU applies the 'manifestly inappropriate test' – i.e., a low standard of scrutiny that confers to the EU legislator a huge margin of maneuver in order to the objectives envisaged. On the contrary, in the evaluation of fundamental civil liberties, the CJEU usually recurs to a high standard of analysis. See Takis Tridimas, "The principle of proportionality", in Robert Schütze and Takis Tridimas, *op. cit.*, pp. 243-264, p. 247.

³³⁹ See the Opinion of Advocate General Mengozzi, *Opinion 1/15*, 8 September 2016, EU:C:2016:656, para. 205, according to whom strict necessity allows '[...] ascertaining whether the contracting parties have struck a 'fair balance' between the objective of combating terrorism and serious transnational crime and the objective of protecting personal data and respecting the private life of the persons concerned'. However, the possibility

*Eifert v Land Hessen*³⁴⁰, the CJEU was called upon to balance the individuals' fundamental rights to privacy and to the protection of personal data with the general interest in publishing the names of people benefitting from the European Agricultural Guarantee Fund and the European Agricultural Fund for Rural Development³⁴¹. The CJEU maintained that neither the Council of the EU nor the European Commission demonstrated that they had taken into account other methods of publishing the information '[...] which would be consistent with the objective of such publication while at the same time causing less interference with those beneficiaries' right to respect for their private life in general and to protection of their personal data in particular, such as limiting the publication of data by name relating to those beneficiaries according to the periods for which they received aid, or the frequency or nature and amount of aid received'³⁴². In other words, the co-legislators should have evaluated the possibility that a limited publication – as described by the CJEU – may have been sufficient to achieve the objectives pursued by the EU legislation. The arguments brought by the European Commission to justify the enhancement of the degree of harmonisation of Member States' legislations through the GDPR were very poor and, in any case, it could not justify the necessity and proportionality of its intervention³⁴³. More clearly articulated was the justification brought by the European Commission to substitute the Council Framework Decision 2008/977/JHA of 27 November 2008 (DPFD)³⁴⁴ by enforceable measures with

to envisage another less intrusive mean should be sufficiently effective to attain the objective pursuit compared with the one offered under the agreement.

³⁴⁰ C-92/09 and C-93/09, *Volker und Markus Schecke GbR, Hartmut Eifert v Land Hessen*, 9 November 2010, EU:C:2010:662.

³⁴¹ The 'disclosure' of personal data, indeed, shall be considered as a data processing activity according to Opinion of the Article 29 DPWP No. 5/2001 on *the European Ombudsman Special Report to the European Parliament following the draft recommendation to the European Commission in complaint 713/98/IJH*, Brussels, 17.05.2001.

³⁴² C-92/09 and C-93/09, *Volker und Markus Schecke GbR, Hartmut Eifert v Land Hessen*, para. 83. In the same judgment the CJEU clarified that the proportionality principle shall be differently balanced as for legal persons since the GDPR only applies in case the business name allows the identification of one or more physical persons. Hence, the CJEU estimated that legal persons were already subject to gravest burdens in the publication of the data so that imposing to national authorities the revision of the business names of all the company's beneficiary of the European Agricultural Guarantee Fund and the European Agricultural Fund for Rural Development would have been disproportionated (para. 87). In C-620/19, *Land Nordrhein-Westfalen v D.-H.T.*, 10 December 2020, EU:C:2020:1011, the CJEU declared itself not competent to interpret Article 23 GDPR as transposed internally by the German law on the freedom of information of 27 November 2011, since its scope of application was enlarged so as to include legal person that are not contemplated under EU law.

³⁴³ See the Proposal for Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25.1.2012, para. 2.3.: 'The principle of proportionality requires that any intervention is targeted and does not go beyond what is necessary to achieve the objectives. This principle has guided the preparation of this proposal from the identification and evaluation of alternative policy options to the drafting of the legislative proposal'.

³⁴⁴ Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, pp. 60-71, that is analysed *infra*.

direct effect regarding the Member States' legal orders³⁴⁵. The EDPS explained that a new package was the most appropriate solution, as Article 16 TFEU improved the data protection field at the Treaty level, while seeking a uniform level of protection throughout the EU³⁴⁶. In the EDPS' view:

‘[...] a single instrument which is directly applicable in the Member States, is the most effective means to protect the fundamental right to data protection and to create a real internal market where personal data can move freely and where the level of protection is equal independently of the country or the sector where the data are processed’³⁴⁷.

In the data protection field necessity and proportionality justify the compliance of the legislative proposals with the standards set forth in the EU data protection *acquis*³⁴⁸. For this reason, the European Commission justifies its proposals in light of the CFREU – namely Articles 7, 8 and 52(1) – more so than with regard to the intensity of its action which, as a last resort, takes its justification from the first paragraph of Article 16 TFEU, rather than the second³⁴⁹. Necessity and proportionality are strictly interpreted in the light of the interference that the legislative proposal causes to the individuals' fundamental rights to the protection of personal and, eventually, to privacy. Both rights can be derogated according to the parameters set forth in Article 52(1) of the CFREU so that:

- first, any restriction should be provided by law;
- second, the essence of the fundamental right shall be respected;
- third, the limitations shall genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others, and
- fourth, the measure shall be necessary and proportionate to be acceptable in any democratic society³⁵⁰.

³⁴⁵ See, for example, the German position requiring an evaluation of the DPFJ justifying the need of the adoption of a new Directive in the Council of the EU, *Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data - Chapters V-VI*, 6846/14 ADD 3, Brussels, 28 March 2014, p. 4.

³⁴⁶ Opinion of the EDPS on *the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"*, Brussels, 14.01.2011.

³⁴⁷ *Ibid.*, p. 15.

³⁴⁸ In this sense, see the Assessment of the EDPS on *the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, Brussels, 11.04.2017.

³⁴⁹ Further reflections have been made by Charlotte Bagger Tranberg, "Proportionality and data protection in the case law of the European Court of Justice", *International Data Privacy Law*, Vol. 1, No. 4, 2011, pp. 239-248, highlighting the use of the strict necessity test in the data retention field.

³⁵⁰ It can be noted that also in emergency situations, as the one overcome during the COVID-19 pandemic, data subject rights cannot be derogated beyond the limits set forth by Article 52(1) of the CFREU as underlined by the EDPB, "Thirtieth Plenary session: EDPB response to NGOs on Hungarian Decrees and statement on Article 23 GDPR", *Press Release*, Brussels, 3.06.2020.

Thus, the strict necessity test represents the last step of the evaluation of the lawfulness of any legislative measure interfering with the individuals' fundamental right to the protection of personal data. Yet the CJEU takes into account all the requisites foreseen by Article 52(1) CFREU – either in order, or out of order – to assess whether a breach to Article 8 of the CFREU has occurred.

First, any restriction must be established by law³⁵¹ – including an international agreement³⁵² – on which data controllers can rely on:

‘In particular, the domestic law must be sufficiently clear in its terms to give citizens an adequate indication of the circumstances in and conditions under which controllers are empowered to resort to any such restrictions’³⁵³.

In *Smaranda Bara*, the CJEU assessed whether the right to be informed had been respected with regard to the exchange of personal data from the Romanian National Tax Administration Agency to the National Health Insurance Fund³⁵⁴. The CJEU found that the data that had been transferred aimed at identifying insured persons and, consequently, the data subjects should have been informed if the limitations of Article 13 DPD had not applied³⁵⁵. Although the possibility to derogate from this obligation was contemplated under Article 11(2) DPD, the CJEU recalled that this should be laid down by law in full respect of the principle of legality. Concretely, this principle ensures the respect of the principles of necessity and proportionality so law must set forth ‘[...] clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse’³⁵⁶. As a result, the CJEU found a

³⁵¹ Note that according to Article 57(1)(c) GDPR, national legislator shall consult the supervisory authority before adopting a legislative measure restricting individuals' subjective rights.

³⁵² *Opinion 1/15*, paras. 142-147.

³⁵³ Guidelines of the EDPB No. 10/2020 on *restrictions under Article 23 GDPR. Version 1.0*, Brussels, 15.12.2020, p. 7.

³⁵⁴ C-201/14, *Smaranda Bara and Others v Preşedintele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală (ANAF)*, 1 October 2015, EU:C:2015:638. The CJEU highlighted that both the transfer of data and the subsequent processing by the National Health Insurance Fund should be classified as processing of personal data in the light of Article 2(a) DPD (para. 29). The former transferred personal data to the latter in order to enable it to require the payment of arrears of contribution to the health insurance regime by virtue of an internal protocol. The applicant challenged the fact that the mentioned protocol did not require the data subject to be informed so as to express the consent on the transfer of data from the National Tax Administration Agency to the National Health Insurance Fund, which constituted a further processing.

³⁵⁵ The CJEU recalled that the processing of data not obtained from the data subject imposes to the data controller to inform the data subject on the purposes of the processing and the categories of data concerned according to Article 11(1)(b) and (c) DPD.

³⁵⁶ C-201/14, *Smaranda Bara and Others v Preşedintele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală (ANAF)*, para. 176. See, also, C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, para. 109: ‘That legislation must, in particular, indicate in what

breach of Article 13(1)(e) and (f) DPD since, although this allowed Member States to restrict the scope of the right to information for ‘an important economic or financial interest of a Member State [...], including monetary, budgetary and taxation matters’ or ‘a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e)’, such a limitation was neither foreseen by Romanian national law, nor by the internal protocol that legitimises the transfer of data from one administration to the other³⁵⁷. The CJEU echoed its founding in *Digital Rights Ireland*, in which it said:

‘[...] the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance’³⁵⁸.

In addition, Article 52(1) CFREU requires that any restriction respects the ‘essence of fundamental rights’. The principle of the essence of a fundamental right is an open concept that the CJEU often confuses with those of necessity and proportionality³⁵⁹. At first sight, we could allege that only those principles codified under Article 8 of the CFREU represent the “essence” of the right to the protection of personal data. However, when it comes to evaluating the necessity and proportionality of a specific legislative measure, the CJEU takes into account other principles and rules following the ECtHR’s jurisprudence³⁶⁰ and the EU’s data protection *acquis*³⁶¹. In its historical sentence on Directive 2006/24/EC of 15 March

circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary [...].’

³⁵⁷ C-201/14, *Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF)*, para. 45. Yet, according to Article 11 GDPR, the data subject should have been informed of the further processing process, the identity of the controller and of his representative, if any, and any further information – e.g., categories of data concerned, recipients, the existence of the right to access and to rectify the data.

³⁵⁸ C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014, EU:C:2014:238, para. 37.

³⁵⁹ Opinion of Advocate General Cruz Villalón, C-650/13, *Thierry Delvigne/Commune de Lesparre Médoc and Préfet de la Gironde*, 4 June 2015, EU:C:2015:363, paras. 115 y 116. Note that in the data protection field the CJEU successfully separates the analysis of the essence of the fundamental right to an effective remedy enshrined in Article 47 of the CFREU from the test of the strict proportionality as it is testified by judgment C-311/18, *Data Protection Commissioner/ Facebook Ireland Ltd, Maximillian Schrems*, 16 July 2020, ECLI:EU:C:2020:559, paras. 181 and 182. Concretely, the essence of Article 47 of the CFREU is related to the broader principle of governance of the rule of law for which the state is accountable for its actions before an authority that meets the requirements of independence and impartiality. See Kathleen Gutman, “The essence of the Fundamental Right to an Effective Remedy and to a fair Trial in the Case-Law of the Court of Justice of the European Union: The Best is Yet to Come”, *German Law Journal*, Vol. 20, No. 6, 2019, pp. 884-903.

³⁶⁰ As it is maintained by the Opinion of the Article 29 DPWP No. 01/2014 on the “*Application of necessity and proportionality concepts and data protection within the law enforcement sector*”, Brussels, 27.02.2014.

³⁶¹ As laid down in the Explanations relating to the Charter of Fundamental Rights, OJ C 303, 14.12.2007, pp. 17-35.

2006 (Data Retention Directive)³⁶², *Digital Rights Ireland*³⁶³, the CJEU observed that the Directive did not undermine the essence of Articles 7 and 8 of the CFREU since the content of the communication was not registered and in light of the safeguards on data protection and data security ensured therein – at least as far as the accidental or unlawful destruction, accidental loss, or alteration of data is concerned. According to the CJEU:

‘Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because Article 7 of Directive 2006/24 provides, in relation to data protection and data security, that, without prejudice to the provisions adopted pursuant to Directives 95/46 and 2002/58, certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks. According to those principles, Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data’³⁶⁴.

Similarly, in *Opinion I/15* Advocate General Mengozzi specified that the EU-Canada PNR draft Agreement was deemed to respect the essences of the fundamental rights to privacy and to the protection of personal data since the data collected was limited to the air travellers between Canada and the EU, and provided that the draft Agreement set forth relevant safeguards to protect the integrity and security of the data³⁶⁵. However, there are few judgments in which the CJEU refers to the ‘essence of the fundamental right’ to the protection of personal data which leave an aura of uncertainty about the core of Article 8 CFREU. Moreover, the references to data security ‘raises questions as to [its] role [...] vis-à-vis the protection of the fundamental right’³⁶⁶. Surely data security is not contemplated among the principles and rules listed in Article 8 of the CFREU. As Hustinx highlights, the essential elements³⁶⁷ embedded in Article 8 are the ‘key principles’ of the DPD, but:

‘[...] it cannot be excluded that the Court of Justice might find other main elements of data protection which have not been expressed in Article 8(2) and (3), but are available in Directive 95/46/EC and may be seen as implied in Article 8(1) of the Charter. Such elements might also help to reinforce the elements which have already been made explicit and further develop the impact of the general right expressed in Article 8(1)’³⁶⁸.

³⁶² Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJL* 105, 13.4.2006, pp. 54-63.

³⁶³ C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, paras. 26 to 82.

³⁶⁴ *Ibid.*, para. 40.

³⁶⁵ Opinion of Advocate General Mengozzi, *Opinion I/15*, para. 186.

³⁶⁶ Irene Kamara, *op. cit.*, p. 56.

³⁶⁷ Matteo E. Bonfanti, *op. cit.*, p. 447, affirms that they represent a sort of “minimum indispensable” necessary to the define the essence of the right to the protection of personal data.

³⁶⁸ Peter Hustinx, 2017, *op. cit.*, p. 140.

Among these ‘other elements’ we should recall the following principles and rules.

- The principle of data minimisation³⁶⁹ for which the processing of personal data shall be ‘adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed’³⁷⁰. This includes data protection by design and by default principles that direct the application of data protection safeguards to the design and development of any system or product that is intended to process personal data³⁷¹.
- The categories of personal data processed include a general prohibition of processing special categories of personal data³⁷², including data on health, ethnic origin, religious beliefs³⁷³, and biometrics³⁷⁴. Specifically, in *Opinion 1/15* the CJEU affirmed that sensitive data should have not been used for automated comparison with risk assessment criteria or databases³⁷⁵ which, in any case, require an *ex post* human control³⁷⁶ and a monitoring mechanism administered by the national supervisory authority³⁷⁷ to avoid any discriminatory results³⁷⁸.
- The principle of storage limitation imposes that data shall be processed ‘[...] no longer than is necessary for the purposes for which the personal data are processed’, unless ‘[...] for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes [...]’³⁷⁹. Specific safeguards must be taken into account depending on the nature, scope and purposes of the processing or categories of processing³⁸⁰.

³⁶⁹ Article 5(1)(c) GDPR.

³⁷⁰ Article 5(1)(c) GDPR.

³⁷¹ Preliminary Opinion of the EDPS No. 5/2018 on *privacy by design*, Brussels, 31.05.2018, p. 1. See also: the Opinion of the EDPS on *Promoting Trust in the Information Society by Fostering Data Protection and Privacy*, Brussels, 18.03.2018, para. 42; the Spanish Agency on Data Protection, *A Guide to Privacy by Design*, Madrid, 2019, and the Recommendation of the Article 29 DPWP No. 1/99, Brussels, 23.02.1999.

³⁷² Article 9 GDPR: ‘data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation’. Also, digital images can be considered to be special categories of personal data as far as it is processed to derive special categories of data. See the Opinion of the Article 29 DPWP No. 02/2012 on *facial recognition in online and mobile services*, Brussels, 22.03.2012, p. 4.

³⁷³ *Opinion 1/15*, para. 167.

³⁷⁴ Articles 4(14) GDPR: ‘means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data’.

³⁷⁵ *Opinion 1/15*, para. 174.

³⁷⁶ *Ibidem*.

³⁷⁷ Advocate General Mengozzi, *Opinion 1/15*, para. 256.

³⁷⁸ *Opinion 1/15*, para. 174.

³⁷⁹ Article 5(1)(e) GDPR.

³⁸⁰ Advocate General Mengozzi, *Opinion 1/15*, para. 284, maintained that the duration of a five-year period of all the air passengers travelling between the EU and Canada period could have not been justified in the light of the strict necessary principle since, on one hand, some data was directed to other purposes than combatting of terrorism and serious crime and, on the other one, this data was retained for a subsequent period of two years.

- The right of data subjects to be informed about the restriction placed upon their rights according to the principle of transparency³⁸¹, unless that may be prejudicial to the purpose of the restriction. The information shall be provided in writing, or by other means, including, where appropriate, electronically³⁸² and it must be easily accessible and understandable to the data subject, which requires special attention regarding the language of the information and the individual (or data subject) to whom the information is addressed.
- The right to the erasure of personal data³⁸³, the right to restriction of processing³⁸⁴, and the right to object to the processing of personal data³⁸⁵. The right to erasure of personal data – also known as the right to be forgotten – was formulated by the CJEU in the case of *Google Spain*³⁸⁶. On that occasion, the CJEU confirmed that the applicant had the right to have his/her personal data erased – and, as consequence, the right to object to the processing – before Google Spain that, unlike other editors, could not benefit from the clause of processing of data for journalistic purposes. The right to restriction of processing can be invoked in case of inaccurate, unlawful, disproportionate, or fully automated individual decision-making process and limits the processing activities to: the data subject's consent; the establishment, exercise or defence of legal claims; the protection of the rights of another natural or legal person, or for reasons of important public interest for the Union or of a Member State. The right to object is directed at ceasing the processing of personal data that, although lawful, is based on specific circumstances pertaining to the data subject³⁸⁷. In case of

In practice, PNR data could have been 'unmasked' – i.e., depersonalised – to identify travellers also for investigative purposes after the passenger left the Canadian's territory.

³⁸¹ See the Opinion of the EDPS No. 3/2015, *Europe's big opportunity. EDPS recommendations on the EU's options for data protection reform*, Brussels, 27.07.2015, p. 8.

³⁸² Article 12(1) GDPR.

³⁸³ Article 16 GDPR.

³⁸⁴ Article 18 GDPR.

³⁸⁵ Article 21(1) GDPR as far as the data processing activities realised on the basis of points (e) and (f) of Article 6 GDPR.

³⁸⁶ C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González*, 13 May 2014, EU:C:2014:317. The case concerned the request by Mr. Costeja González to Google to remove or alter the web pages resulting by inserting his name in the search engines. The webpage, indeed, offered a series of links to other webpages – especially to the Spanish newspaper La Vanguardia – containing announcements of Mr. Costeja González for a real-estate auction connected with attachment proceedings for the recovery of social security debts. Information that, according to Mr. Costeja González, was obsolete since those proceedings had already been resolved. See also C-136/17, *GC, AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL)*, where the CJEU analysed the request to de-reference various links leading to web pages published by third parties following a search conducted through Google's search engine with the applicants' names.

³⁸⁷ The right to object may lead to the erasure of personal data, but its scope is stricter: while the former applies to all the lawful grounds of processing set forth under Article 6 GDPR, the latter is limited to those cases where

objection, and pending the verification of the lawfulness of the activity, the data subject is granted the right to restriction of processing³⁸⁸ under which the data can be processed only for limited reasons like for ‘reasons of important public interest of the Union or of a Member State’³⁸⁹.

- The principles of security, integrity, and confidentiality of personal data³⁹⁰ that prevent abuse or unlawful access or transfer. Integrity and confidentiality are a concretisation of the principle of security in personal data processing activities. The integrity principle aims at avoiding accidental or malicious unlawful alteration of the information and also at prohibiting the linkage of data; confidentiality seeks to prevent any unlawful access to the data by unauthorised authorities which can be ensured by security features – e.g., pseudonymisation and encryption.
- The explicit appointment of the controller or categories of controllers³⁹¹ whose role consists in the explanation of why and how personal data is processed³⁹². Data controllers are not necessarily empowered by the law but, in practice, they must be in charge of determining the purposes and means of processing. The data controller may be a legal entity³⁹³ acting on behalf of a private company or a public body, or a

the processing is conducted by public authorities only. If the objection succeeds, the controller shall erase the data in the light of Article 17(1)(c) read in conjunction with Article 21(1) GDPR.

³⁸⁸ See Article 18(1)(d) GDPR.

³⁸⁹ See Article 18(2) GDPR.

³⁹⁰ Concretely, confidentiality requires that any person acting under the authority of data controller or processor (including the latter) must not process personal data unless it is required to do so by the data controller itself, or by provision of law as it occurs in case of disclosure of personal data to law enforcement authorities to prevent, investigate, detect, or persecute criminal offences or to execute criminal penalties. Furthermore, confidentiality requires that data enabling the re-identification of data subjects is kept separate from other personal data thanks to the use, for example, of a cryptographic algorithm that is especially recommended to capture and transfer biometric templates through the Internet. See Article 5(1)(f) GDPR, and Oksana Frolova, “EU Role in Ensuring International Information Security”, *Scientific Annals of Alexandru Ioan Cuza University of Iasi: Political Science*, 2019, Vol. 14, No. 1, pp. 89-102.

³⁹¹ See Article 4(7) GDPR. The authority acting on behalf of the controller, the so-called data processor according to Article 4(8) GDPR, might be delegated specific tasks especially concerning the means through which data are processed, such as the guarantee of the principles of confidentiality and security. See the Opinion of the Article 29 DPWP No. 1/2010 *on the concepts of "controller" and "processor"*, Brussels, 16.02.2010.

³⁹² See the Opinion of the Article 29 DPWP No. 3/2010 *on the principle of accountability*, Brussels, 13.07.2010, and Lee A. Bygrave and Luca Tosoni, “Article 4(7): Controller”, in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *op. cit.*, pp. 145-156. The authors highlight that the determination of the purpose for processing is the major criteria to point out as far as data controller accountability is concerned, which is also manifested by exercising its influence or participation in the determination of the data processing purposes. We shall also highlight that data controllers must be able to demonstrate that the data subject has provided the consent in a freely way – see Article 7(4) GDPR.

³⁹³ C-272/19, *VQ v Land Hessen*, 9 July 2020, EU:C:2020:535.

group of individuals³⁹⁴ which gives rise to the concept of “joint accountability”. It is not relevant whether the controller/s has/have access to the data or not³⁹⁵.

- The risks to the rights and freedoms of data subjects may require evaluation with regard to the principles of necessity and proportionality through an impact assessment³⁹⁶. An impact assessment is required, for example, in case of large-scale processing of special categories of data³⁹⁷, such as biometrics or personal data relating to criminal convictions and offences³⁹⁸, or when data processing activities concern the systematic monitoring of a publicly accessible area on a large scale.
- The scope of the restrictions introduced – i.e., which rights that are restricted and how far they are limited.

Article 23 GDPR³⁹⁹ establishes an exhaustive list of cases where a data subject’s rights⁴⁰⁰ can be restricted and fills out⁴⁰¹ the vague concept of ‘general interest’ required by Article

³⁹⁴ C-25/17, *Tietosuojavaltuutettu*, 10 July 2018, EU:C:2018:551.

³⁹⁵ In C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, 29 July 2019, EU:C:2019:629, the CJEU sentenced that a data controller cannot be responsible for the activity realised before and after its own when it does determine neither the objective nor the means.

³⁹⁶ On the development of a risk-based approach in the data protection field see the Statement of the Article 29 DPWP on *the role of a risk-based approach in data protection legal frameworks*, Brussels, 30.05.2014, that points out how several dispositions of the GDPR are built upon this logic, namely: Articles 22, 23, 28, 30, 33, 38, and 39 GDPR. According to the Guidelines of the Article 29 DPWP on *Data Protection Impact Assessment (DPIA) and determining whether processing is ‘likely to result in a high risk’ for the purposes of Regulation 2016/679*, Brussels, 4.04.2017, the controller is called on to do such an evaluation, for example, when the processing contemplates a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and the decision taken has legal effects on the natural person or similarly significantly affects the natural person.

³⁹⁷ Article 9(1) GDPR.

³⁹⁸ Article 10 GDPR.

³⁹⁹ See the Guidelines of the EDPB No. 10/2020 on *restrictions under Article 23 GDPR. Version 1.0*, Brussels, 15.12.2020.

⁴⁰⁰ Namely, those enshrined in Articles 12 to 22 GDPR, that is: the principle of transparency (Article 12), the right to information (Articles 13 and 14), the right to access (Article 15), the right to rectification (Article 16), the right to erasure (Article 17), the right to restriction of processing (Article 18), the right to notification in case of rectification or erasure of personal data or restriction of processing (Article 19), the right to data portability (Article 20), the right to object (Article 21), the right not to receiving automated individual decision-making, including profiling (Article 22), the communication of data breach (Article 34), and the principle relating to the data processing (Article 5). Also, the rights set forth in Article 34 GDPR, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22 GDPR, can be limited.

⁴⁰¹ Among these, reasons of: national security; defence; public security, that includes ‘[...] protection of human life, especially in response to natural or manmade disasters’ – see recital (73) GDPR, and the Guidelines of the EDPB No. 10/2020 on *restrictions under Article 23 GDPR. Version 1.0*, Brussels, 15.12.2020, p. 8; the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security; the protection of judicial independence and judicial proceedings; the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g) of Article 23(1); the protection of the data subject or the rights and freedoms of others, and the enforcement of civil law claims.

52(1) of the CFREU. In *Digital Rights Ireland*⁴⁰², for example, the CJEU found that the storage of data by telecommunication service providers according to the Data Retention Directive was appropriate to attain the objective of the prevention, investigation, detection, and persecution of serious crimes. However, its scope of application, covering almost the entire population of Europe, failed the requirement for strict necessity⁴⁰³ so that the Data Retention Directive had to be invalidated. The CJEU put into evidence that the data retained affected all people notwithstanding the fact that they might be related to a situation subject to criminal persecution or not, and that the Data Retention Directive applies '[...] even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime'⁴⁰⁴.

Specifically, the CJEU evaluated a series of issues and considerations: the data retention period that did not distinguish between different categories of data on the basis of their usefulness with regard to the purpose for which it was obtained; the provision of data security measures to prevent the risk of abuse as well as unlawful accesses; the quantity of data; the sensitive nature of the data; the risk of unlawful access that undermined the integrity and confidentiality of the data stored, and the lack of prohibitions on transfers of data to third countries. Furthermore, the CJEU complained about the lack of an *ex ante* scrutiny by a court or an independent administrative body over the competent national authorities with access to the data⁴⁰⁵.

In *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert, Immo 9 SPRL, Grégory Francotte*⁴⁰⁶, the CJEU was requested to evaluate if the activity of a private detective acting for a professional body in charge of investigating ethics breaches would have fallen within one of the exceptions provided for by the DPD and, concretely, under the clause on prevention, investigation, detection, and prosecution of criminal offences⁴⁰⁷. The CJEU noted that in cases where Member States had transposed those provisions in their national law, professional bodies and their private detectives could have relied on exceptions. These exceptions included the data subject not being informed at the time of the

⁴⁰² C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, paras. 26 to 82.

⁴⁰³ *Ibid.*, para. 56.

⁴⁰⁴ *Ibid.*, para. 58.

⁴⁰⁵ *Ibid.*, paras. 60-62.

⁴⁰⁶ C-473/12, *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert, Immo 9 SPRL, Grégory Francotte*, 7 November 2013, EU:C:2013:715.

⁴⁰⁷ Alternatively, it was proposed to underpin the exception on the protection of the data subject or on the rights and freedoms of others – see respectively Article 13(1)(d) or (g) DPD, now points (d) and (i) of Article 23 GDPR.

processing of the personal data. When such provisions had not been transposed in the national order, the Member State itself should have evaluated if, according to internal law, the obligation to inform the data subject could have been derogated or not – e.g., in case such an omission justified the exercise of public authorities’ functions.

The *Schrems* judgments⁴⁰⁸ are also noteworthy. In *Maximillian Schrems v Data Protection Commissioner* the CJEU evaluated the lawfulness of the self-certification mechanism referred to as Safe Harbour Principles through which US organisations should have adhered to a European Commission Decision 2000/520/EC of 26 July 2000⁴⁰⁹ and the relevant Annexes for enabling the transfer of personal data⁴¹⁰. The CJEU pointed out that self-certified organisations could have derogated from them for reasons of national security, public interest, or law enforcement and, as a result, EU data subjects could have suffered from interferences without any guarantee that the authorities would be limit their activity and without access to an effective legal remedy. Therefore, the CJEU maintained that the principle of strict necessity had been breached because: the storage of personal data was transferred to the US without any differential, limitation, or exception as for the objective pursued; the lack of objective criteria to limit the access to personal data by public authorities, as well as its subsequent processing for specific purposes that should have been restricted, and that should have been proportionally justified according to the interference⁴¹¹. Finally, the European Commission failed to comply with the DPD principles because of the lack of any guarantee ensuring the right to rectification or erasure of data, as well as the right to an effective judicial remedy. After the invalidation of the Safe Harbour Principles, the CJEU analysed in *Data Protection Commissioner v Facebook Ireland Ltd. and Maximillian Schrems* the accomplishment of the EU-US Privacy Shield Act in the light of the provisions set forth in the CFREU read in conjunction with the GDPR. The EU-US Privacy Shield Act also left an open clause through which the principles guarantying the protection of fundamental rights could have been derogated for reasons of national security, public interest, or law enforcement requirements. As a result, the CJEU claimed that EU data was

⁴⁰⁸ C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015, EU:C:2015:650, and C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd. and Maximillian Schrems*, 16 July 2020, EU:C:2020:559.

⁴⁰⁹ Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance), *OJ L* 215, 25.8.2000, pp. 7-47.

⁴¹⁰ Greer Damon, “Safe harbor—a framework that works”, *International Data Privacy Law*, No. 1, Vol. 3, 2011, pp. 143-148, highlights that Safe Harbour significantly contributed to raise the level of privacy compliance in the US, though recognising that such a mechanism was “not perfect”.

⁴¹¹ C-362/14, *Maximillian Schrems v Data Protection Commissioner*, para. 93.

held hostage by the US surveillance programs PRISM and Upstream. The communication, retention, and access to transferred EU data constituted an interference with regard to Articles 7 and 8 of the CFREU, whose legality should have been assessed in the light of its Article 52(1). Both US programmes were found to be contrary to the principle of proportionality as they conferred unlimited powers to the US intelligence services without granting effective and enforceable rights in cases of abuse. The CJEU then turned to Article 47 of the CFREU and the guarantee of an effective judicial remedy in the third country, this being one of the parameters contemplated by the European Commission in its adequacy decisions⁴¹². The Privacy Shield Ombudsperson, that was not a judicial organisation, was estimated to be not independent in the exercise of its tasks given that its mandate was dependent on the Secretary of State and the US State Department. Moreover, neither was this authority empowered to adopt binding decisions on the intelligence services nor could have data subjects relied on other political remedies⁴¹³.

Another crucial judgment where the principle of proportionality played a leading role concerned the ePrivacy Directive, that is, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*⁴¹⁴. While applying the test of the ‘strict necessity’, the CJEU noted that:

‘[the] legislation provides for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication, and that it imposes on providers of electronic communications services an obligation to retain that data systematically and continuously, with no exceptions [...]’⁴¹⁵.

The CJEU observed that the systematic retention of traffic and location data subverted the logic of the ePrivacy Directive that clearly establishes the retention of data for criminal purposes as an exception and not a general rule. The huge amount of data retained allowed for the deriving of precise information on individuals that might have not been connected to the committing of a criminal offence. Provided that they were not informed of the processing of their data, a feeling of being under constant surveillance was spreading, according to the CJEU. The CJEU stressed that to ascertain whether the national authorities’ access to data is limited to what is strict necessity, a preventive control conducted by a judge, or an independent administrative authority is essential – except in cases of justified urgency⁴¹⁶.

⁴¹² Art. 45(2)(a) GDPR.

⁴¹³ Art. 45(7) GDPR.

⁴¹⁴ See C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*.

⁴¹⁵ *Ibid.*, para. 97.

⁴¹⁶ *Ibid.*, para. 119:

Such a decision should come from a reasoned request submitted by the competent authority that seeks to access the data, especially in the fields of the prevention, investigating and exercise of criminal action. In any case, the data subject should be informed of the processing of his/her data unless this would undermine the investigations conducted by the national authority. Finally, the CJEU stated that given the huge amount of data stored, its nature, and the risk of unlawful access, the data should not be disclosed outside the EU and must be destroyed once the retention period expired.

Notably, in *Privacy International*⁴¹⁷, the CJEU highlighted that national security, as established under Article 4(2) TEU, legitimises interferences with individuals' fundamental rights that are more serious than those applicable in the pursuit of other objectives⁴¹⁸. In these cases, the legislative measure regulating such interference shall also lay down appropriate substantive and procedural rules in order to comply with the strict necessity test. This is not the case with generalised and undifferentiated disclosure of traffic and location of data that concern the totality of people using electronic communication systems, including of those people for which there is neither an indirect or remote link with the purpose of safeguarding national security nor the proved existence of a relationship between the disclosure of data and the threat to national security⁴¹⁹. The same reasoning – i.e., that serious crimes allow for serious interference⁴²⁰, while preventing, investigating, detecting, and

‘[...] In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime [...]. However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities’.

⁴¹⁷ C-623/17, *Privacy International*, 6 October 2020, EU:C:2020:790, where the CJEU was called to assess the compatibility of Article 94 of the British Telecommunications Act of 1984 – for which to security and intelligence services – with Articles 7, 8, 11 and 52(1) of the CFREU.

⁴¹⁸ *Ibid.*, para. 75.

⁴¹⁹ *Ibid.*, para. 80. In the same line, the CJEU did not exclude from the scope of application of DPD in the light of Article 2(a) the data contained in a list of the Slovakian Financial Directorate and the Finance and Crime Office of financial administration – see C-73/16, *Peter Puškár v Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy*. The CJEU maintained that the list was drafted for collecting taxes and combatting tax fraud and not for the purpose of pursuit criminal proceeding in the frame of the State's criminal activity. Furthermore, Article 13(1)(e) DPD expressly provided for the possibility to restrict data subjective rights in safeguard an important economic or financial interest of a Member State or of the EU, including monetary, budgetary and taxation matters. As a consequence, a limitation of data protection for tax purposes should be considered to be comprised by the DPD.

⁴²⁰ For example, the CJEU covered the preventive storage of Internet Protocol addresses to fight crimes and safeguard public security since, although constituting a serious interference with the individuals' fundamental rights, it may constitute the sole tool of investigation that allows the identification of the person whose Internet Protocol address was attributed to the commitment of an online crime, such as child pornography, in C-511/18, C-512/18 and C-520/18, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, v Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées*, para. 154.

prosecuting criminal offences in general terms allows less serious interferences⁴²¹ – was supported by the CJEU in *La Quadrature du Net*⁴²², where the Court of Luxembourg was asked to analyse under what terms the processing of traffic, location, Internet Protocol address, and civil identity data stored for the purposes of national or public security, falling within the scope of Article 15(1) of the ePrivacy Directive, could have been considered to be proportionate with regard to Articles 7 and 8 of the CFREU⁴²³. At this point, the CJEU recalled that an effective control by a judicial or independent administrative authority is needed and that this body should be empowered to issue a binding decision to assess the existence of prejudicial situations that impose harsher restrictions and guarantees⁴²⁴.

A final remark should be made regarding the necessary and proportionate test *vis-à-vis* the requisite of ‘necessity in a democratic society’. From the ECtHR jurisprudence we understand that the proportionality test circumscribed to the concept of necessity in a democratic society encompasses the identification of the proportionate response to a specific pressing social need that includes the evaluation of the public concern or the nature of the issue to be tackled⁴²⁵. This is not a requisite set forth in Article 52(1) CFREU, but the CJEU could invoke it on the basis of the dialogue between it and the ECtHR. In *Privacy International*, for instance, the CJEU recalled that the ePrivacy Directive aims at establishing

⁴²¹ The CJEU estimated that the preventive storage of data related to civil identity did not constitute a serious interference since it does not give any information on the individuals’ private life so that national measures allowing the storage of and access to civil identity aimed at identifying the internet user, can be justified in the light of the prevention, research, ascertaining, and persecution of general crimes as mentioned by Article 15(1), first sentence, ePrivacy Directive, *ibid.*, paras. 138 and 139.

⁴²² C-511/18, C-512/18 and C-520/18, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d’accès à Internet associatifs, Igwan.net, v Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l’Intérieur, Ministre des Armées*.

⁴²³ *Ibid.*, para. 135: ‘[...] in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilizing the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities’. The same conclusions were reached in C-140/20, *G.D. v Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General*, 5 April 2022, EU:C:2022:258, para. 101. In the latter judgment, the CJEU recalled that targeted measures of retention of location data are based on geographic criterion, like the average crime rate, which circumscribes the investigation area without infringing the prohibition of discrimination (para. 80).

⁴²⁴ *Ibid.*, paras. 138 and 139. In C-746/18, *H. K., Prokuratuur*, 2 March 2021, EU:C:2021:152, the CJEU found that the public prosecutor who directs the investigation and, eventually, the prosecution proceedings cannot be recognised as having the status of a third party in relation to the legitimate interests at stake, since it is in charge of submitting the dispute to the competent court, as a party to the proceedings in which the prosecution takes place (paras. 55-57). In the same line, the CJEU denied the independent character of a police officer when s/he processes the requests to access the data stored by electronic communication services, even though s/he is assisted by a unit set up within the police which enjoys a degree of autonomy in the exercise of its tasks whose decisions may subsequently be subject to judicial review – see C-140/20, *G.D. v Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General*, para. 114.

⁴²⁵ Recital (73) GDPR. As it is maintained by the Opinion of the Article 29 DPWP No. 01/2014 on the “Application of necessity and proportionality concepts and data protection within the law enforcement sector”, Brussels, 27.02.2014.

a high level of confidentiality for electronic communications so that, in principle, it is prohibited to disclose information to third parties, including the storage of data, as well as to security and intelligence services. However, Article 15(1) of the ePrivacy Directive allows for some form of derogation:

‘[...] where this constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence and public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system’⁴²⁶.

3.2. Article 16 of the Treaty on the Functioning of the European Union as a horizontal but sectorial competence: The case of the Area of Freedom, Security and Justice

Because of its ties with the internal market project, the DPD promoted the adoption of sectorial regulations to protect personal data in other domains⁴²⁷. For example, the ePrivacy Directive and the Data Retention Directive were adopted as far as telecommunications were concerned, and the eCommerce Directive, while the e-signature Directive⁴²⁸ covered commercial fields⁴²⁹.

The Justice and Home Affairs Area (JHA Area) was excluded from the DPD⁴³⁰ and from the ECDPR as their scope of application was limited to the European Community only⁴³¹. Although the Amsterdam Treaty shifted the EU administrative competences from the third to the first pillar⁴³² and, therefore, they fall within the scope of the DPD and the ECDPR⁴³³

⁴²⁶ C-623/17, *Privacy International*, para. 58.

⁴²⁷ The Committee of Ministers Recommendation R (87) 15 regulating *the use of personal data in the police sector*, Strasbourg, 17 September 1987, para. 2, already recognised that a sectorial approach to data protection had been promoted thanks to the issuing of several recommendations on: automated medical data banks, scientific research and statistics, direct marketing, and social security purposes.

⁴²⁸ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, *OJ L* 13, 19.1.2000, pp. 12-20, repealed by Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, *OJ L* 257, 28.8.2014, pp. 73-114.

⁴²⁹ Communication from the Commission to the European Parliament and the Council, Way forward on aligning the former third pillar acquis with data protection rules, COM(2020) 262 final, Brussels, 24.6.2020.

⁴³⁰ Article 3(2), first paragraph, DPD: ‘[...] in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in the areas belonging to criminal law’. See the Article 29 DPWP, *Second Annual Report*, Brussels, 30.11.1998, p. 29, that specifically refers to the Convention on the establishment of a European Police Office (Europol Convention), *OJ C* 316, 27.11.1995, pp. 2-32, and to the Council of the EU, *Eurodac Convention*, Brussels, 28/29.V.1998, for asylum seekers’ fingerprints, as fields falling outside the DPD.

⁴³¹ Council of the EU, *IGC 2003 – Non-institutional issues; including amendments in the economic and financial field*, ICG 37/03, Brussels, 24 October 2003, p. 5.

⁴³² Which was not previously forbidden since Member States could have incorporated the DPD with a sectorial approach – see its recital (23).

⁴³³ See the Article 29 DPWP, *Third Annual Report*, Brussels, 22.12.2000, p. 53: ‘[...] these areas of activity come within the scope of the directive and when drafting new Community instruments under Title IV of the

contrary to the desire of some Member States⁴³⁴, Titles V and VI of the 1997 TEU on the CFSP and on the PJCCM⁴³⁵ respectively were retained under the intergovernmental roof. Yet, several instruments had been agreed during the '90s to enable the access to, and exchange of information among, the Member States in order to fight terrorism and to ensure security within the EU. Among others, we recall that the Europol, the Eurojust, the processing of personal data within the SIS⁴³⁶, and the CIS all adhere to their own set of rules on the protection of personal data, which makes Hijmans and Scirocco noting that:

‘As a result, in the context of the EU, data protection has changed from an internal market issue to become a broader concern. The main legal and political debates in recent years do not concern internal market issues but relate to the complex relation between data protection and the activities of the State to ensure security’⁴³⁷.

The fact that each instrument had its own set of rules with regard to the protection of personal data in compliance with the ECHR’s legal framework⁴³⁸ resulted in a “patchwork” of fragmented and unsatisfactory legislations which paid scant attention to the protection of the fundamental rights dimension⁴³⁹. As a result, EU policies on PJCCM have represented

EC Treaty this must be taken into account’. At the same page, it is recalled the Italian’s paper aimed at examining the possibility to adopt a uniform approach also for third pillar’s measures, see the Council of the EU, *Discussion paper on the protection of personal data in the Third Pillar of the EU*, 5643/99, Brussels, 4 February 1999.

⁴³⁴ The extension to data protection legislation to sensible policy, as it is the migration one, was not pacifically accepted by the Member States that reluctantly extended such safeguard to third country nationals, especially irregular migrants. This aspect is confirmed by Diana Alonso Blas, “First Pillar and Third Pillar: Need for a Common Approach on Data Protection?”, in Serge Gutwirth, Yves Pouillet, Paul De Hert, Cécile de Terwangne, and Sjaak Nouwt, *Reinventing Data Protection?*, The Netherlands, Springer, 2009, pp. 225-237, p. 231, and it will come out when we analyse the evolution of large-scale IT systems in Chapter III, to which we refer.

⁴³⁵ See Articles 2(d) and (e) of the DPD for which data controller and processor may also be a public authority. Meanwhile, Member States’ laws on the protection of personal data in the law enforcement fields had been adjusted to Convention 108 as: ‘The application of Convention 108 is therefore not limited to the first pillar, as it is the Directive; in fact the pillars are an ‘EU invention’, not a Council of Europe one. Actually, the Convention plays a fundamental role in the third pillar sector’ – Diana Alonso Blas, *op. cit.*, p. 226.

⁴³⁶ Flanking measures were adopted under the Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, *OJ L 239*, 22.9.2000, pp. 19-62 (Convention implementing the Schengen Agreement hereinafter) and, despite their ancillary label, occupied the majority of its dispositions as highlighted by Lode Van Outrive, “Historia del Acuerdo y del Convenio Schengen”, *Revista CIDOB d’Afers Internacionals*, No. 53, 2001, pp. 46-61, and David O’Keeffe, “The Schengen Convention: A Suitable Model for European Integration?”, *Yearbook of European Law*, No. 1, Vol. 11, 1991, pp. 185-219, Vendelin Hreblay, *La libre circulation des personnes: les accords Schengen*, Paris, Les Éditions G. Crès et Cie, 1994, and Id., *Les accords de Schengen: origine, fonctionnement et avenir*, Brussels, Bruylant, 1998.

⁴³⁷ Hielke Hijmans and Alfonso Scirocco, *op. cit.*, p. 1493.

⁴³⁸ Article 6(1) TEU. As Franziska Boehm, *op. cit.*, p. 11, points out:

‘One important vehicle to limit the use of police and judicial power is a high data protection standard. It is therefore in the interest of both the individuals and the actors of the police and the judiciary, whose work is much more tolerated when the rights of individuals are respected, to find a balance between police and judicial needs and the rights of the individuals’.

⁴³⁹ On the contrary, second pillar measures completely lack a data protection legal framework since, differently from Article 30(1)(b) of the 1997 TEC that expressly called for exchange and protection of data, no provision was established in the 1997 TEU.

the hardest obstacle to reaching a whole, comprehensive approach to data protection as the various organisations seek to prevent, investigate, detect, persecute criminal offences as well as to execute criminal penalties, all of which are activities that could potentially restrict the individual's fundamental private sphere⁴⁴⁰. Because of the Member States' reluctance to confer powers regarding criminal law to the EU, data protection regulations for PJCCM purposes had not been created until recently.

3.2.1. The protection of personal data for police and judicial cooperation in criminal matters: Still a patchwork?

With the Hague Programme of 2005⁴⁴¹, the Council of the EU proposed the formalisation of the principle of availability of information in a Framework Decision that would enable direct access to all, or specific data held by the other Member States – i.e., 'index data' that could be searched through the European Police Records Index System (EPRIS). This principle would ensure that information was put at the reciprocal disposal of the Member States⁴⁴² and was defined as follows:

‘The information that is available to certain authorities in a Member State must also be provided to equivalent authorities in other Member States. The information must be exchanged as swiftly and easily as possible between the authorities of the Member States and preferably by allowing direct online access’⁴⁴³.

The principle of availability is coloured by different modalities of information sharing⁴⁴⁴. First, 'equivalent access' allows indirect access to the information stored by another Member State upon request and only under the principle of reciprocity as regulated in the Convention

⁴⁴⁰ Paul De Hert, 2016, *op. cit.*, p. 112. The author points out that the narrowly interpretation given by the CJEU to individuals' fundamental rights, for example in C-399/11, *Stefano Melloni v Ministerio Fiscal*, 26 February 2013, EU:C:2013:107, and C-396/11, *Ciprian Vasile Radu*, 2 January 2013, EU:C:2013:39, may seriously undermine the higher level of protection ensured to individuals in the Member States' constitutions while giving priority to the execution of EU law, namely the European Arrest Warrant. On the matter, see Pablo Jesús Martín Rodríguez, "Tribunal Constitucional -- Sentencia 26/2014, de 13 de febrero, en el recurso de amparo 6922-2008 promovido por Don Stefano Melloni", *Revista de Derecho Comunitario Europeo*, No. 18, Vol. 48, 2014, pp. 603-622, and Id., "Crónica de una muerte anunciada: Comentario a la Sentencia del Tribunal de Justicia (Gran Sala) de 26 de febrero de 2013, Stefano Melloni, C-399/11", *Revista General de Derecho Europeo*, No. 30, 2013, pp. 1-45.

⁴⁴¹ The Hague Programme: strengthening freedom, security and justice in the European Union, *OJ C 53*, 3.3.2005, pp. 1-14.

⁴⁴² *Ibid.*: '[...] a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirement of ongoing investigations in State'.

⁴⁴³ See the Opinion of the EDPS on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005) 490 final), (2006/C 116/04), Brussels, 17.05.2006, para. 16.

⁴⁴⁴ See Tony Bunyan, "The principle of availability: the free market in access to data/intelligence will rely on "self-regulation" by the law enforcement agencies and make accountability almost meaningless", *StateWatch*, 2006, available at www.statewatch.org.

on Mutual Assistance in Criminal Matters between Member States of the EU⁴⁴⁵, or through the Council Framework Decision 2006/960/JHA of 18 December 2006⁴⁴⁶ (the Swedish Initiative). Second, the Prüm Treaty of 27 May 2005 allows the direct query of national systems for specific types of data in a two-step approach⁴⁴⁷: a search of the index reveals whether the information on the person or object searched is available or not (hit/no-hit mechanism) and, in case of a positive match in the index, the requesting Member State shall apply an appropriate legal instrument that regulates the cooperation among law enforcement or judicial authorities that will receive the relevant data⁴⁴⁸. Third, the Council Framework Decision 2009/315/JHA of 26 February 2009⁴⁴⁹ – that gave rise to the European Criminal Record System (ECRIS)⁴⁵⁰ – introduces a form of availability based on a non-request model in which Member States commit to exchange information on a convicted person to the Member State of his/her nationality. Finally, the European Investigative Order⁴⁵¹ enables a

⁴⁴⁵ See Article 6(1) *in fine* of the Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union - Council Declaration on Article 10(9) - Declaration by the United Kingdom on Article 20, *OJ C* 197, 12.7.2000, pp. 3-23.

⁴⁴⁶ Confront Article 5 of the Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, *OJ L* 386, 29.12.2006, pp. 89-100. Notably, the Swedish Initiative is also used for the exchanging data in the frame of Asset Recovery Offices according to Council Decision 2007/845/JHA, *OJ L* 332, 18.12.2007, p. 103.

⁴⁴⁷ Convention on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, signed in Prüm on 27 May 2005, entered into force on 1 November 2006. The Treaty has been extended to all the Member States through its institutionalisation by the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, *OJ L* 210, 6.8.2008, pp. 1-11 (Prüm Decision hereinafter).

⁴⁴⁸ Opinion of the European Data Protection Supervisor on the Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Slovenia, the Slovak Republic, the Italian Republic, the Republic of Finland, the Portuguese Republic, Romania and the Kingdom of Sweden, with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, *OJ C* 169, 21.7.2007, pp. 2-14, para. 9:

‘[...] Although the initiative must be seen as an implementation of this principle, it does not lead to availability as such but it is only one further step towards availability of law enforcement information across the borders of the Member States. It is part of a piecemeal approach aiming to facilitate the exchange of law enforcement information’.

⁴⁴⁹ Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, *OJ L* 93, 7.4.2009, pp. 23-32. However, it also contemplated the possibility to request information in the frame of a criminal proceeding or other purposes – confront its Article 6.

⁴⁵⁰ Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, *OJ L* 93, 7.4.2009, pp. 33-48.

⁴⁵¹ Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *OJ L* 130, 1.5.2014, pp. 1-36.

requesting Member State to ask another state to collect, store, and transmit evidence ‘even if this is not yet available in the national jurisdiction’⁴⁵².

In 2005, the European Commission submitted a Proposal for a Framework Decision on the principle of availability⁴⁵³, and a Proposal for a Council Framework Decision on the protection of personal data⁴⁵⁴. Although the European Commission had to drop the former initiative⁴⁵⁵, the latter was adopted shortly before the entry into force of the Lisbon Treaty. The DPDF was unanimously agreed upon within the Council, without the European Parliament’s involvement, on the basis of Articles 30(1)(a) and 30(b) of the 2002 TEU⁴⁵⁶. The DPDF wanted to draw Member States’ data protection legislations closer in the law enforcement and criminal judicial fields while granting a high level of public security⁴⁵⁷. Yet, the level of protection granted therein was far less satisfactory than that established by the DPD, the Convention 108⁴⁵⁸, and the Recommendation (87) 15 of the Council of

⁴⁵² See the Opinion of the EDPS on *the initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the French Republic, the Italian Republic, the Republic of Hungary, the Republic of Poland, the Portuguese Republic, Romania, the Republic of Finland and the Kingdom of Sweden for a Directive of the European Parliament and of the Council on the European Protection Order, and - on the initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the Republic of Austria, the Republic of Slovenia and the Kingdom of Sweden for a Directive of the European Parliament and of the Council regarding the European Investigation Order in criminal matters*, Brussels, 5.10.2010, para. 15.

⁴⁵³ See the Proposal for a Council framework decision on the exchange of information under the principle of availability, COM(2005) 0490 final, Brussels, 12.10.2005.

⁴⁵⁴ Proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, COM(2005) 0475 final, Brussels, 4.10.2005.

⁴⁵⁵ Communication from the Commission to the European Parliament and the Council - Consequences of the entry into force of the Treaty of Lisbon for ongoing interinstitutional decision-making procedures, COM(2009) 0665 final, Brussels, 2.12.2009. The consultation procedure requiring the unanimity of the delegations sit in the Council of the EU was crippled at least since 2006 when the EDPS issued his comment – see the Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability, COM(2005) 490 final, *OJC* 116, 17.5.2006, pp. 8-17. Some reflections on the difficult integration of the PJCCM policies are made by Claudia Jiménez, “La lucha de la UE contra el actual crimen organizado: un reto esencial...pero difícil”, *Revista CIDOB d’Afers Internacionals*, No. 111, 2015, pp. 35-56.

⁴⁵⁶ Specifically, Article 30(1)(b) of the 2002 TEU allowed the European Community to adopt measures on ‘the collection, storage, processing, analysis and exchange of relevant information, including information held by law enforcement services on reports on suspicious financial transactions, in particular through Europol, subject to appropriate provisions on the protection of personal data’.

⁴⁵⁷ For an analysis of the DPDF’s rules applied to Union databases, see Javier Valls Prieto, *Problemas jurídicos penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial*, Madrid, Dykinson, 2017, p. 43 ff. A first Proposal for a Council framework decision, COM(2005) 0475 final, Brussels, 4.10.2005, was discarded as negotiations turned out to be rather hard. See the Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision establishing the European Police Office (Europol), COM(2006) 817 final, 30.12.2010, para. 13.

⁴⁵⁸ See the Second Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, *OJC* 91/9, 24.4.2007, para. 4 in fine, and the Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on an area of freedom, security and justice serving the citizen, *OJC* 276/8, 17.11.2009, paras. 29-33.

Europe⁴⁵⁹, as the DPF⁴⁶⁰ contemplated broad provisions that were adaptable in case of urgent need on the part of law enforcement⁴⁶¹. First of all, and although it aimed at approximating national legislations⁴⁶², the DPF⁴⁶³ neither had direct effect on the Member States' legal orders, nor could it be brought under the scrutiny of the CJEU, both of which prevented any harmonisation of the Member States' domestic legislations⁴⁶⁴. Secondly, lacking the European Commission infringement powers in cases of non-transposition, the application of the DPF⁴⁶⁵ was hampered by the Member States' inertia⁴⁶⁶. The DPF⁴⁶⁷ was limited to cross-border processing activities – also for transferring personal data to third countries and international organisations⁴⁶⁸ – and was not involved in activities occurring within a sole Member State⁴⁶⁹. It expressly excluded from its scope the Council Framework Decision 2005/222/JHA⁴⁷⁰, and⁴⁷¹:

‘Several acts, adopted on the basis of Title VI of the Treaty on European Union, contain specific provisions on the protection of personal data exchanged or otherwise processed pursuant to those acts. [...] The relevant set of data protection provisions of those acts, in particular those governing the functioning of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS), as well

⁴⁵⁹ Hielke Hijmans and Alfonso Scirocco, *loc. cit.*, highlight Article 11(d) on the principle of purpose limitation.

⁴⁶⁰ Cristina Blasi Casagran, *Global Data Protection in the Field of Law Enforcement: An EU perspective*, Abingdon, Routledge Research in EU Law, 2017, p. 43.

⁴⁶¹ Article 34 of the 1997 TEU.

⁴⁶² Steve Peers, “EU Justice and Home Affairs Law (Non-Civil)”, in Paul Craig and Gráinne de Búrca, *The Evolution of EU Law*, Oxford, Oxford University Press, 2011, pp. 272-274, highlights that framework decisions and decisions constituted the great achievement of the Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, *OJ C* 340, 10.11.1997, pp. 1-144, that conserved from the previous Maastricht Treaty only conventions and common positions. With regard to the formers, he observes that:

‘[...] the Council was attracted to the great efficiency ruling by these measures, since they did not have to be ratified as such by national parliaments in order to take effect [...] A number of pre-Amsterdam Joint Actions and conventions were replaced by framework decisions and decisions. The phasing out of new conventions and the replacement of prior Conventions means that national parliaments no longer had a power of approval over the main Third Pillar acts, although in many cases national parliaments tried to maintain influence in this area by insisting on scrutiny reserves, which delayed the formal adoption of measures by did not appear to have any significant on the content of any measures’.

⁴⁶³ Which should have not been underestimated since the European Commission undertook infringement procedure for the non-transposition of the DPD already in 1999 – see the Recommendation of the Article 29 DPWP No. 1/2000 on *the Implementation of Directive 95/46/EC*, Brussels, 3.02.2000. The situation changed with the entry into force of the Lisbon Treaty according to the provisions set forth in Protocol No 36 on transitional provisions, *OJ C* 115, 9.5.2008, pp. 322-326.

⁴⁶⁴ Article 13(2) DPF.

⁴⁶⁵ Recitals (7)-(9) and Article 1(2) DPF and Paul De Hert and Vagelis Papakonstantinou, “The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters — A modest achievement however not the improvement some have hoped for”, *Computer Law & Security Review*, No. 25, 2009, pp. 403-414, p. 403.

⁴⁶⁶ Recital (37) DPF and Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *OJ L* 69, 16.3.2005, pp. 67-71.

⁴⁶⁷ Article 1(1). See the Council of the EU, *Efforts to harmonise the protection of personal data in the third pillar of the EU*, 9084/1/99, Brussels, 11 June 1999. Notably, Diana Alonso Blas, *loc. cit.*, maintains that it was not desirable to adapt the Europol's regime on data to the DPF since the former was more protective than the latter.

as those introducing direct access for the authorities of Member States to certain data systems of other Member States, should not be affected by this Framework Decision. The same applies in respect of the data protection provisions governing the automated transfer between Member States of DNA profiles, dactyloscopic data and national vehicle registration data pursuant to the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime⁴⁶⁸.

The DPF⁴⁶⁹’s scope was limited to those acts that had been adopted under Title VI TEU and had data protection rules that were ‘more limited in scope’, unless the provisions were more restrictive than those contained in DPF⁴⁷⁰. Therefore, the DPF did not set standard rules on the protection of personal data for the PJCCM and, as far as EU institutions and bodies were concerned, it did not complement the ECDPR⁴⁷¹. All in all, the DPF did not repeal the existing dispositions that were already binding Member States: The Convention 108, its First Additional Protocol of 2001, and the Council of Europe conventions on judicial cooperation in criminal matters remained unaffected⁴⁷².

Suppressing the Greek pillar structure and conferring to the EU a crosscutting competence on personal data, the Lisbon Treaty was expected to abandon the sectoral approach to data while informing the founding treaties with a sole (critical) exception: the CFSP⁴⁷³. The horizontal position of Article 16 TFEU was thought to enable the EU to overcome numerous, inconsistent, and overlapping dispositions⁴⁷³ while embracing data processing activities both

⁴⁶⁸ Recital (39) DPF.

⁴⁶⁹ Recital (40) DPF.

⁴⁷⁰ Recital (36) DPF.

⁴⁷¹ Confront recital (41) DPF.

⁴⁷² Article 16(3) TFEU leaves unaffected 39 TEU according to which:

‘In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities’.

However, no decision has been adopted so far which leaves uncovered the delicate issue of the protection of the individual’s fundamental rights *vis-à-vis* international sanctions: C-402/05 P and C-415/05 P, *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities*, 3 September 2008, EU:C:2008:461; T-85/09, *Kadi v Commission*, 30 September 2010, paras. 157 and 177, and C-584/10 P, C-593/10 P, and C-595/10 P, *European Commission and Others v Yassin Abdullah Kadi*, 18 July 2013, EU:C:2013:518. See also the opinions of the EDPS on *the proposal for a Council Regulation amending Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban*, (2009/C 276/01), Brussels, 17.11.2009, and the one on *various legislative proposals imposing certain specific restrictive measures in respect of Somalia, Zimbabwe, the Democratic Republic of Korea and Guinea*, (2010/C 73/01), Brussels, 23.3.2010. Also, see the letter of the EDPS on *three legislative proposals concerning certain restrictive measures*, Brussels, 20.07.2010, namely with regard to Mr. Milosevic and persons associated with him, in support of the mandate of the International Tribunal for the Former Yugoslavia, and in respect of Eritrea.

⁴⁷³ Joint contribution of the Article 29 DWP on *the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, Brussels, 1.12.2009.

in the private and in the public sector⁴⁷⁴. The EU intervention in the AFSJ was promoted by the Information Management Strategy⁴⁷⁵ presented as part of the Stockholm Programme of 2 December 2009⁴⁷⁶ and developed within the European Information Exchange Model. As the European Commission stated:

‘We need to strengthen the EU’s stance in protecting the personal data of the individual in the context of all EU policies, including law enforcement and crime prevention as well as in our international relations’⁴⁷⁷.

The principles of ‘consistency and comprehensiveness’⁴⁷⁸ worked in favour of an approach whereby regulations would set out the general rules on data protection. Specifically, the DPFD could have been replaced by a new instrument adopted under the ordinary legislative procedure with direct effect within the Members States’ legal orders⁴⁷⁹. The European Commission strategy of 2012 on personal data protection attempted to gather all the activities related to new sources of data stemming from globalisation and new technologies under one roof⁴⁸⁰, but the plan failed. Two different Proposals were

⁴⁷⁴ It can be pointed out the Article 29 DPWP’s comment on the proposal of the 2012 data protection package where it clearly pointed out how the simultaneous regulation of private and public domains provides for broad expectations to privacy rights for reasons of public interest that significantly lowered the guarantees set forth compared to the private sector – Opinion of the Article 29 DPWP No. 01/2012 on *the data protection reform proposals*, Brussels, 23.03.2012, p. 12.

⁴⁷⁵ See the Communication from the Commission to the European Parliament and the Council, Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM), COM(2012) 0735 final, Brussels, 7.12.2012, in which the European Commission analysed four instruments to exchange information (the Swedish Initiative, the Prüm Decision, Europol, and the SIS) and three existing channels of communication (the Supplementary Information Request at the National Entries (SIRENE), the Secure Information Exchange Network Application (SIENA) that connects the Europol National Units, and the I-24/7 communication tool of the Interpol). Member States should have implemented a Single Point of Contact to gather all the law enforcement authorities with access to the national databases, including SIRENE Bureau, Europol National Units, and Interpol National Central Bureaux. See the Opinion of the EDPS on *the Communication from the Commission to the European Parliament and the Council entitled ‘Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM)’*, Brussels, 29.04.2013, p. 6.

⁴⁷⁶ See Council of the EU, *The Stockholm Programme – An open and secure Europe serving and protecting the citizens*, 17024/09, Brussels, 2 December 2009, and correlated documents: the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2010) 171 final, Brussels, 20.4.2010; the Communication from the Commission to the European Parliament and the Council, Overview of information management in the area of freedom, security and justice, COM(2010) 0385 final, Brussels, 20.7.2010. Confront the Opinion of the EDPS on *the Communication from the Commission to the European Parliament and the Council – “Overview of information management in the area of freedom, security and justice”*, Brussels, 30.09.2010, para. 19, and previously, the Green Paper on detection technologies in the work of law enforcement, customs and other security authorities, COM(2006) 474 final, Brussels, 1.9.2006.

⁴⁷⁷ *Ibid.*, p. 3.

⁴⁷⁸ See the Opinion of the EDPS on *the data protection reform package*, Brussels, 7.03.2012, p. 6.

⁴⁷⁹ Hielke Hijmans and Alfonso Scirocco, *op. cit.*, p. 1519. In the same line, the authors called for a legislative framework developing Article 39 TEU – i.e., data protection in the CFSP – for which: one instrument should be bounding the EU Institutions, and another one the Member States.

⁴⁸⁰ See the Opinion of the EDPS on *the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – “A comprehensive approach on personal data protection in the European Union”*, Brussels, 14.01.2011.

submitted⁴⁸¹ to safeguard a special regime for PJCCM⁴⁸² in the light of Declaration No 21 attached to the Lisbon Treaty:

‘[...] specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields’.

In addition, Declaration No 20 was taken into account as the rules on the protection of personal data that ‘could have direct implications for national security’ were intentionally excluded from the DPD and from any subsequent legislation. To conclude, processing activities on personal data for the PJCCM were left out of the GDPR⁴⁸³ and were regulated under a new directive, the LED. This implied that a binding instrument, enforceable by individuals and subject to the scrutiny of the CJEU, entered into force in 2016⁴⁸⁴. Similarly, the new EUDPR, repealing the ECDPR, provides a specific Chapter, IX, that covers the processing activities regarding “operational personal data”⁴⁸⁵ carried out by Union bodies, offices and agencies under Chapter 4 or 5 of Title V of part three TFEU. The LED and the EUDPR were adopted on the basis of Article 16 TFEU as the ‘protection of personal data’ foreseen under Article 30(1)(a) of the 2002 TEU⁴⁸⁶ had been suppressed and replaced by the new Article 87(2)(a) TFEU⁴⁸⁷. Therefore, Article 16(2) TFEU was found to be the correct

⁴⁸¹ Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 011 final - 2012/0011 (COD). The Opinion of the Article 29 DPWP No. 01/2012 on *the data protection reform proposals*, Brussels, 23.03.2012, p. 5, expressed disappointment for this choice while highlighting that:

‘The Working Party notes the fact that the Commission has chosen to present a separate proposal for a Directive applicable to the area of police and criminal justice due to political constraints. A high level of consistent data protection standards also applying to this area is all the more needed. In any case, it should be clear that the new Directive must not result in Member States lowering their current data protection standards set for the police and criminal justice sector’.

A similar position was maintained in the Opinion of the EDPS on *the data protection reform package*, Brussels, 7.03.2012, p. 4.

⁴⁸² *Ibidem*.

⁴⁸³ Notably, the Article 29 DPWP underlined that data protection principles were applicable to the PJCCM by virtue of Article 8 of the CFREU notwithstanding the limited scope conferred of the DPD in the Opinion of the Article 29 DPWP No. 01/2014 on *the "Application of necessity and proportionality concepts and data protection within the law enforcement sector"*, Brussels, 27.02.2014, p. 13.

⁴⁸⁴ The Kingdom of Spain has already been condemned for its non-transposition – see C-658/19, *European Commission v Kingdom of Spain*, 25 February 2021, EU:C:2021:138.

⁴⁸⁵ See Chapter IV of our dissertation.

⁴⁸⁶ Previously, Article K.3 of the 1992 TEU established that: ‘In the areas referred to in Article K.1, Member States shall inform and consult one another within the Council with a view to coordinating their action. To that end, they shall establish collaboration between the relevant departments of their administrations’.

⁴⁸⁷ Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 010 final, Brussels, 25.1.2012:

legal basis to regulate the protection of personal data and the free movement of such data for the PJCCM, too.

a) The scope of the Law Enforcement Directive

Although the LED was drawn up on the basis of the protective skeleton of the GDPR, many of its provisions diverge from the latter under the aegis of greater exceptionalism⁴⁸⁸. First of all, the scope of the LED is limited to processing activities performed by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of, threats to public security⁴⁸⁹. These authorities are broadly described as⁴⁹⁰:

- any public authority responsible for the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against, and the prevention of, threats to public security, or
- any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of, threats to public security.

Therefore, the LED applies only in presence of both an objective and subjective element⁴⁹¹. The LED imposes on the data controller the need to distinguish to which subject the data processed belongs to – i.e., suspect or non-suspect⁴⁹² – and to separate personal data

‘The proposal is based on Article 16(2) TFEU, which is a new, specific legal basis introduced by the Lisbon Treaty for the adoption of rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. The proposal aims to ensure a consistent and high level of data protection in this field, thereby enhancing mutual trust between police and judicial authorities of different Member States and facilitating the free flow of data and co-operation between police and judicial authorities’.

⁴⁸⁸ Ma Isabel Gonzalez Cano, “Transfer and Treatment of Personal Data in the Criminal Process: Progress and Immediate Challenges of the Directive (EU) 2016/680”, *Revista Brasileira de Direito Processual Penal*, Vol. 5, No. 3, 2019, pp. 1331-1384.

⁴⁸⁹ Article 1(1) LED.

⁴⁹⁰ Article 3(7) LED.

⁴⁹¹ Juraj Sajfert and Teresa Quintel, “Data protection directive (EU) 2016/680 for police and criminal justice authorities”, *SSRN Electronic Journal*, 2017, pp. 1-22, p. 4, noting that Member States may extend its scope of application to “minor offences” according to recital (12) LED.

⁴⁹² See recital (31) and Article 6 LED plus the Opinion of the Article 29 DPWP No. 01/2013 *providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive*, Brussels, 26.02.2013, p. 3. According to them, data subjects must be distinguished and, specifically, these may be: persons with regard to whom there are serious grounds for believing that they have committed or are about to

based on facts from personal data obtained through personal assessments⁴⁹³. However, the creation of a rigid categorisation of personal data during an investigation or a criminal trial has been criticised, since it may be detrimental for the individuals affected until the circumstances surrounding the case at stake have been fully explored⁴⁹⁴.

The principle of lawfulness enshrined in the LED is vaguer than that of the GDPR and takes distance from requiring the data subject's consent. Article 8(1) LED sounds as follows:

‘Member States shall provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law’.

As a result, the LED requires Member States to specify the objectives of processing, the personal data to be processed, and the purposes of the processing, while discarding the need for the data subject to give consent through law⁴⁹⁵. Subsequent processing of personal data by the ‘same or another controller’⁴⁹⁶ for the purposes covered by the LED – including reasons different than those for which the data had been collected – are allowed if: the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law, and the processing is necessary and proportionate to the new purpose in accordance with Union or Member State law⁴⁹⁷. Also, subsequent processing is allowed for ‘archiving in the public interest, scientific, statistical or historical use’⁴⁹⁸. Thus, the wording used by the LED leaves open the possibility to process personal data for other purposes, notwithstanding whether these are compatible or not with the initial purpose⁴⁹⁹. The lack of any provision on the consent of the data subject and on the wide interpretation

commit a criminal offence; persons convicted of a criminal offence; victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence, and other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons of the two former categories

⁴⁹³ Article 7(1) LED.

⁴⁹⁴ Mark Leiser and Bart Custers, “The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680”, *European Data Protection Law Review*, Vol. 5, No. 3 2019, pp. 367-378, p. 375.

⁴⁹⁵ *Ibid.*, p. 374.

⁴⁹⁶ Paul De Hert and Juraj Sajfert, “The fundamental right to personal data protection in criminal investigations and proceedings: framing big data policing through the purpose limitation and data minimization principle of the Directive (EU) 2016/680”, *Brussels Privacy Hub Working Paper*, Vol. 7, No. 31, 2021, pp. 14-17, p. 11:

‘As we already said, further processing, in the GDPR meaning of the term, can only be done by the same controller on the same legal basis. Once data are transmitted to another controller, or the same controller starts using a different legal basis, the processing begins ab novo, with the initial processing - collection of data, followed by informing the data subject pursuant to provisions on the right of information (Articles 13 and 14 GDPR) etc.’.

⁴⁹⁷ See Article 4(2) LED.

⁴⁹⁸ Article 4(3) LED.

⁴⁹⁹ Which reflects previous Article 11 DPF.

of the principle of purpose limitation were strongly criticised by the Article 29 DPWP since both suspects or convicted persons, and also ‘non suspects’ – such as the victims of human trafficking⁵⁰⁰ – could be affected.

The right to access personal data can be significantly restricted⁵⁰¹, partially or completely⁵⁰², in respect of the limits established under Article 52(1) of the CFREU⁵⁰³, in order to: avoid obstructing official or legal inquiries, investigations or procedures; avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; protect public security; protect national security, and protect the rights and freedoms of others. These restrictions may concern “categories of processing” in which case Member States must outline the categories in national law⁵⁰⁴. Although data controllers are responsible for informing the data subject of a refusal or restriction of access⁵⁰⁵, the LED allows such information to be completely omitted where the provision thereof would undermine a purpose pursued by the competent authorities⁵⁰⁶. Regarding the latter, Article 16 of the LED guarantees the right to rectify and erase personal data as well as the right to restrict processing⁵⁰⁷, but it also exempts data controllers from providing notification of refusal of rectification or erasure of personal data or restriction of processing (and of the reasons for the refusal) to⁵⁰⁸: avoid obstructing official or legal inquiries, investigations or procedures; avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; protect public security; protect national security, or protect the rights and freedoms of others. Again, the sole limit envisaged is set down in the Charter and reads as follows: ‘[...] a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned’. In cases where the rights to access, rectify, and erase personal data as well as the right to restrict processing are refused and the data subject is not, or not fully, informed,

⁵⁰⁰ See the Opinion of the EDPS No. 03/2015 on *the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, Brussels, 1.12.2015, p. 6.

⁵⁰¹ Article 14 LED.

⁵⁰² Article 15(1) LED.

⁵⁰³ See *supra*.

⁵⁰⁴ Article 15(2) LED.

⁵⁰⁵ Article 15(3) LED.

⁵⁰⁶ Article 15(3) LED.

⁵⁰⁷ Article 16(3) LED establishes that the data controller should restrict the processing instead of erase personal data when: the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained or the personal data must be maintained for the purposes of evidence.

⁵⁰⁸ Article 16(4) LED.

the LED establishes that the controller should inform the data subject that they may lodge a complaint with a supervisory authority or seek a judicial remedy⁵⁰⁹. It is important that this information is clearly communicated to the data subject as it is the only legal avenue through which individuals may exercise their rights.

National supervisory authorities, then, play a crucial role, as they supervise⁵¹⁰ and may exercise the data subject's rights as 'an intermediary'⁵¹¹. Notably, under the LED, the competencies of the national supervisory authority may be restricted⁵¹² 'for the supervision of processing operations of courts when acting in their judicial capacity' and 'to supervise processing operations of other independent judicial authorities when acting in their judicial capacity' which avoids a reciprocal monitoring of judicial authorities among the Member States.

Recalling other relevant principles that, although not embedded in Article 8 of the CFREU, are gaining more and more relevance in the data protection field, we can assume that the LED foresees the following exceptions.

- Data must be 'adequate, relevant and not excessive in relation to the purposes for which they are processed'⁵¹³, where the use of the expression 'not excessive' instead of 'limited to what is necessary', used by the GDPR, is more permissible⁵¹⁴.
- This principle of accuracy is mitigated⁵¹⁵ given that inaccurate data may be useful for the persecution, investigation, and prevention of criminal offences. Here, the data controller may refuse to rectify or erase personal data, or restrict its processing⁵¹⁶ when it is not clear that the data subject is fully informed of the underlying reasons as to why the data was collected⁵¹⁷.

⁵⁰⁹ Articles 15(3) and 16(5) LED. According to Juraj Sajfert and Teresa Quintel, 2017, *op. cit.*, p. 5: '[...] those chapters may be perceived as weakening the overall level of protection given to data subjects in EU law and offering too much leeway to police and criminal justice authorities, compared to the remainder of the public sector covered by the GDPR'.

⁵¹⁰ Article 17 LED.

⁵¹¹ Juraj Sajfert and Teresa Quintel, 2017, *op. cit.*, p. 13.

⁵¹² Article 45(2) LED.

⁵¹³ Article 4(1)(c) LED.

⁵¹⁴ Paul De Hert and Juraj Sajfert, *op. cit.*, p. 13: 'There is no need to demonstrate the strict necessity of the data by limiting oneself to the necessary minimum. The controllers under the LED can operate with less precision, they can grab and hold on to data in a rougher manner. They just have to make sure not to process excessive datasets'.

⁵¹⁵ See Articles 4(1)(d), 7(2) and 16(4) LED.

⁵¹⁶ Article 16(3) LED establishes that instead of erasure, the data controller can restrict the processing of personal data when: the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained, or the personal data must be maintained for the purposes of evidence.

⁵¹⁷ Article 16(4) LED directs to the Member States to guarantee the right to lodge a complaint with a supervisory authority or to seek a judicial remedy. Moreover, when the right to information, access,

- Data must be ‘kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed’⁵¹⁸. Article 5 of the LED foresees that ‘Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed’.
- There is no prohibition on processing special categories of data – as it was recommended by the Article 29 DPWP⁵¹⁹ – but these categories can be processed only ‘when strictly necessary’ and under one of the following conditions: under the authorisation of EU or a Member States’ law; to protect the vital interests of the data subject or of another natural person, or where such processing relates to data which is manifestly made public by the data subject.
- Decisions based solely on automated processing, including profiling, are prohibited only if it ‘produces an adverse legal effect concerning the data subject or significantly affects him or her’⁵²⁰. This prohibition can be lifted if ‘Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller’⁵²¹. In a part of departure from the GDPR, the automated processing of special categories of personal data is allowed under the provision that measures to safeguard the data subject’s rights and freedoms and legitimate interests are in place⁵²². In the specific case of profiling⁵²³, this technique is prohibited only in cases where it

rectification, and erasure concerns personal data contained in a judicial decision, a record or case file processed during criminal investigations and proceedings, Member States must shape them according to their legal orders.

⁵¹⁸ Article 4(1)(e) LED.

⁵¹⁹ Opinion of the EDPS No. 03/2015 on *the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, Brussels, 1.12.2015, pp. 8 and 9.

⁵²⁰ Article 11 LED and Lee A. Bygrave, “Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling”, *Computer Law & Security Review*, Vol. 17, No. 1, 2001, pp. 17-24, who finds that legal effects ‘alter or determine a person’s legal rights or duties’.

⁵²¹ Article 11(1) LED.

⁵²² Article 11(2) LED.

⁵²³ Opinion of the EDPS No. 4/2105, *Towards a new digital ethics. Data, Dignity and Technology*, Brussels, 11.09.2015, p. 13:

‘Profiles used to predict people’s behaviour risk stigmatisation, reinforcing existing stereotypes, social and cultural segregation and exclusion, with such ‘collective intelligence’ subverting individual choice and equal opportunities. Such ‘filter bubbles’ or ‘personal echo-chambers’ could end up stifling the very creativity, innovation and freedoms of expression and association which have enabled digital technologies to flourish’.

may result in discrimination and it is based “solely” on special categories of personal data ‘in accordance with Union law’⁵²⁴. In any case, there is no right to access personal data in case of fully automated decision making, including profiling, and such a right is overruled when accessing the information may jeopardise the prevention, detection, investigation, or prosecution of criminal offences⁵²⁵.

- The principles of security, integrity and confidentiality are duly safeguarded, and data must be ‘processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures’⁵²⁶.

b) The first/third pillar dichotomy

Article 9(1) of the LED set forth that personal data processed by competent authorities for non-LED purposes is regulated by the GDPR were authorised by the Union or the national law. The same goes for those processing activities that are entrusted to competent authorities by the Member States’ law and lie outside the scope of the LED⁵²⁷. For example, in case a national police force deploys on public order tasks – as it would, for example, when dealing with the expulsion of illegal migrants –, then, the GDPR and not the LED would be applicable. We believe that, in practice, such a distinction is challenging and might give rise to divergent interpretations in the domestic orders. Indeed, this is not the sole case where the GDPR and LED intertwine. Article 9 of the LED does not incorporate one of the thorniest issues on the GDPR/LED dichotomy, that is, the transfer or access to personal data initially processed by private parties – e.g., telecommunication service providers or carriers – to law enforcement authorities. This topic is mentioned in recital (9) of the LED that states:

‘[...] Regulation (EU) 2016/679 therefore applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to which it is subject. For example, for the purposes of investigation detection or prosecution of criminal offences financial institutions retain certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with Member State law. A body or entity which processes personal data on behalf of such authorities within the scope of this Directive should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to this

⁵²⁴ Article 11(3) LED.

⁵²⁵ Article 15 LED.

⁵²⁶ Article 4(1)(f) LED.

⁵²⁷ Article 9(2) LED.

Directive, while the application of Regulation (EU) 2016/679 remains unaffected for the processing of personal data by the processor outside the scope of this Directive’.

This DPD/DPFD dichotomy was a crucial topic before the Lisbon Treaty entered into force, as European Community and EU measures corresponded to the supranational and the intergovernmental frameworks respectively. Affirming that, as a general rule, the GDPR results applicable in cases where ‘a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to which it is subject’, reflects the CJEU’s jurisprudence on the ePrivacy Directive/Data Retention Directive and on the PNR Agreements. In both cases, the CJEU has maintained a wider interpretation of the DPD so as to include third pillar activities under the first pillar⁵²⁸. This interpretation was justified due to the need to ensure the right to the protection of personal data to individuals and in respect of Article 47 of the 1997 TEU that imposed the preference of first pillar measures over second and third pillars measures⁵²⁹. However, as Hijmans and Scirocco highlight, ePrivacy/Data Retention Directive and PNR Agreements cover slightly different cases, as the data collected by communication service providers is not systematically sent to law enforcement authorities, but rather the authorities are granted access to it on the basis of national law under the “pulled method”⁵³⁰. Hence, while the ePrivacy/Data Retention Directive imposed obligations on private parties only⁵³¹, EU PNR Agreements affected law enforcement authorities too.

In *Ireland v European Parliament and Council of the European Union*⁵³², the CJEU noted that the Data Retention Directive, though first proposed on the basis of Articles 31(1)(c) and

⁵²⁸ See *infra*.

⁵²⁹ Article 47 of the 1997 TEU:

‘Subject to the provisions amending the Treaty establishing the European Economic Community with a view to establishing the European Community, the Treaty establishing the European Coal and Steel Community and the Treaty establishing the European Atomic Energy Community, and to these final provisions, nothing in this Treaty shall affect the Treaties establishing the European Communities or the subsequent Treaties and Acts modifying or supplementing them’.

⁵³⁰ The Opinion of the Article 29 DPWP No. 4/2003 on *the Level of Protection ensured in the US for the Transfer of Passengers’ Data*, Brussels, 13.06.2003, p. 6, and the Opinion of EDPS on *the Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries*, Brussels, 19.10.2010, para. 31, strongly condemn the use of pull system since it creates uncertainties when it comes to apply data protection principles to foreign authorities that do not provide for effective guarantee.

⁵³¹ However, with a significant difference: while the ePrivacy Directive has been conceived as a complementary regulation to the DPD (Article 1(2) of the ePrivacy Directive), the Retention Directive was directed ‘to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime’ (Article 1(1) of the Retention Directive).

⁵³² C-301/06, *Ireland v European Parliament and Council of the European Union*, 10 February 2009, EU:C:2009:68, commented by Orla Lynskey, “The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland”, Vol. 51, No. 6, 2014, pp. 1789-1811. In C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, EU:C:2008:54, 29 January 2008, para. 70, the CJEU had already affirmed that Article 15(1) of the ePrivacy

34(2)(b) of the 1997 TEU as a Framework Decision⁵³³, was correctly underpinned by Article 95 of the 1997 TEC, as it was the measure related to the suppression of obstacles to the internal market by virtue of Article 47 of the 1997 TEU⁵³⁴. Similarly⁵³⁵, in *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*⁵³⁶ the CJEU observed that despite that fact that Article 1(3) of the ePrivacy Directive excluded from its scope the activities concerning public security, defence, state security and those related to areas of criminal law, under its Article 15(1) it allowed the introduction of

Directive allows Member States to introduce a national legislation that imposes to electronic communication service providers to disclose personal data in the frame of a civil proceeding, especially in the light of the effective protection of copyright obliged Member States to set forth such a disposition. The Court then sentenced that it is up to the national judge to balance the fundamental rights at stake in the light of the national laws transposing the above-mentioned Directives.

⁵³³ See the Council of the EU, *Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism*, 8958/04, Brussels, 28 April 2004. Again, the 11-S was the detonating event imposing the systematic retention of telecommunication traffic data, see the adverse Opinion of the Article 29 DPWP No. 5/2002 on the *Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data*, Brussels, 11.10.2002, and the Opinion of the Article 29 DPWP No. 4/2005 on the *Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005)*, Brussels, 21.10.2005, p. 2:

‘Terrorism presents our society with a real and pressing challenge. Governments must respond to this challenge in a way that effectively meets their citizens need to live in peace and security while not undermining their individual human rights – including the right to data privacy– which are a cornerstone of our democratic society’.

⁵³⁴ Jeanne Pia Mifsud Bonnici, “Redefining the Relationship Between Security, Data Retention and Human Rights”, in Ronald L. Holzhaecker, and Paul Luif, *Freedom, Security and Justice in the European Union: Internal and External Dimensions of Increased Cooperation after the Lisbon Treaty*, New York, Springer, 2014, pp. 49-74, p. 51, points out that the Data Retention Directive was firstly proposes as at third pillar framework decision based on Articles 31(1)(c) and 34(2)(b) of the 1997 TEU, yet the lack of unanimity in the Council prevented its adoption:

‘Since it became increasingly clear that unanimity was not possible, the Commission presented, in September 2005, a proposal for a Directive on the retention of data processed in connection with the provision of public electronic communications services and amending Directive 2002/58/EC — the ePrivacy Directive [...] In using a First Pillar solution, member states that were not too keen on blanket data retention measures were still expected to conform. Taking Article 95 EC as the legal basis has been controversial. The choice of legal basis was even questioned before the European Court of Justice (CJEU),¹⁰ with the Court confirming its legality’.

Critics on the communitarisation of a third pillar competence had been raised also by Cathal Flynn, “Data Retention, the Separation of Power in the EU and the Right to Privacy: A Critical Analysis of the Legal Validity of the 2006 Directive on the Retention of Data”, *University College Dublin Law Review*, No. 8, 2008, pp. 1-24.

⁵³⁵ Stephen McGarvey, “The 2006 EC Data Retention Directive: A Systematic Failure”, *Hibernian Law Journal*, No. 10, 2011, pp. 119-171, had advanced an important study on the transposition of the Data Retention Directive in Bulgaria, Romania, Germany, and Ireland so as to warn about potential abuses perpetrated by law enforcement authorities.

⁵³⁶ C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*. The impact of this judgment on national data retention regime is analysed, for example, by Anja Möller Pedersen, Henrik Udsen, and Søren Sandfeld Jakobsen, “Data retention in Europe—the Tele 2 case and beyond”, *International Data Privacy Law*, 2018, Vol. 8, No. 2, pp. 160-174.

derogative provisions on the retention of data, among others, to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or in cases of an unauthorised use of the electronic communication system. Therefore, the CJEU ruled that national law that imposed on electronic communication service providers the duty to retain data on traffic and location for the purpose of criminal law, should be considered to fall under the scope of the ePrivacy Directive⁵³⁷ and, consequently, of the DPD's too⁵³⁸.

In *Privacy International* the CJEU was asked to delimit the scope of the ePrivacy Directive in the light of Article 4(2) TEU that excludes from the EU's competences catalogue measures directed to the safeguarding of public order, internal security, and territorial integrity⁵³⁹. The CJEU recalled that, although Article 4(2) TEU leaves Member States free to determine their policies on internal and external security, this interpretation does not prevent the applicability of EU law and the obligation of Member States to respect individuals' fundamental rights⁵⁴⁰. It made then an important step in outlining the border between the GDPR and the LED by affirming that:

‘[...] where the Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is not covered by Directive 2002/58, but by national law only, subject to the application of [LED], with the result that the measures in question must comply with, inter alia, national constitutional law and the requirements of the ECHR’⁵⁴¹.

Dressing the GDPR/LED dichotomy, the Court confirmed that the processing of personal data should be undertaken by the GDPR when electronic communications service providers firstly process the information for commercial purposes, notwithstanding the fact that the data is then further processed, in terms of transfer or access, by criminal law authorities.

⁵³⁷ See C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, paras. 74 and 75.

⁵³⁸ *Ibid.*, para. 82.

⁵³⁹ Indeed, when ‘national security’ applies *tout court* the legal framework applicable to surveillance activities is made of international law instruments and, concretely, the ECHR. See the Working Document of the Article 29 DPWP on *surveillance of electronic communications for intelligence and national security purposes*, Brussels, 5.12.2014. Here, the Article 29 DPWP warned that national security should be distinguished from other concepts present in the founding Treaties such as security of the EU, state security, public security and defence – specifically, it refers to Article 75 TFEU for the AFSJ, and within the CFSP to Articles 24(1) TEU and 2(4) TFEU. Differently is the situation when a third country invoked national security reasons to obtain personal data processed in the EU. In which case the Article 29 DPWP finds that the EU data protection standards apply except when the national interest of the third states is aligned with the one of a Member State.

⁵⁴⁰ The CJEU could rely on the new GDPR formulations and, specifically, its Articles 2(2)(d) and 23(1)(d) and (h). C-623/17, *Privacy International*, para. 47 *in fine*: ‘It follows that the above interpretation of Article 1(3), Article 3 and Article 15(1) of Directive 2002/58 is consistent with the definition of the scope of Regulation 2016/679, which is supplemented and specified by that directive’.

⁵⁴¹ C-623/17, *Privacy International*, para. 48.

Only when the processing of personal data by the latter authorities is firstly directed to law enforcement purposes does it fall out of the scope of the GDPR⁵⁴² and become regulated under the LED⁵⁴³. This logic is consistent with the new formulation of the GDPR that expressly excludes the activities of:

‘[...] competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security’⁵⁴⁴.

Regrettably, in *Privacy International*, the CJEU did not make any reference to the CFREU, though its application clearly encompasses the PJCCM, too⁵⁴⁵. The Court missed the chance to recall its doctrine on the ‘incorporation’ of fundamental rights for which the EU and its Member States (while implementing EU law) must respect the fundamental right not only while applying EU law, but also when derogating to it⁵⁴⁶.

Turning to the PNR Agreements, instead, the CJEU’s position has been less consistent over the last two decades. In its first judgment, *European Parliament v Council of the European Union and Commission of the European Communities*⁵⁴⁷, the CJEU annulled both the Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the US on the processing and transfer of PNR data by airlines to the US Department of Homeland Security, Bureau of Customs and Border Protection⁵⁴⁸, and the Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data thereto⁵⁴⁹. On that occasion, the CJEU considered that the transfer of PNR data belonged in domain of public security as well as to the Member States’ activity in criminal law and it ruled that the European Community was neither empowered to adopt

⁵⁴² See Article 2(2)(d) GDPR.

⁵⁴³ See also recital (19) GDPR and (11) LED for which public authorities may be subject to one instrument or the other depending on the purposes of their activities.

⁵⁴⁴ Article 2(2)(d) GDPR and Herke Kranenborg, “Article 2: Material scope”, in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *op. cit.*, pp. 60-73, p. 64.

⁵⁴⁵ See Paul De Hert, 2016, *loc. cit.*, and Alexandros Kargopoulos, “Fundamental rights, national identity and EU criminal law”, in Valsamis Mitsilegas, Maria Bergstrom, and Theodora Konstadinides, *op. cit.*, pp. 125-147.

⁵⁴⁶ Paul Craig and Gráinne De Búrca, *EU Law: Text, Cases and Materials*, Oxford, Oxford University Press, 2011, p. 384.

⁵⁴⁷ C-317/04 and C-318/04, *European Parliament v Council of the European Union and Commission of the European Communities*.

⁵⁴⁸ Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, *OJ L* 183, 20.5.2004, p. 83.

⁵⁴⁹ Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection, *OJ L* 235, 6.7.2004, pp. 11-22.

such an Agreement based on Article 95 of the 2002 TEC⁵⁵⁰, nor was it entitled to adopt the corresponding adequacy decision⁵⁵¹. Yet, this judgment was subjected to huge amounts of criticism for leaving considerable uncertainty regarding what the correct legal basis of PNR Agreements was. Despite the promotion of a global approach to PNR Agreements⁵⁵², the EU-Australia PNR Agreement of 2012 was negotiated on the basis of Article 16 TFEU, Article 6 TEU, together with Articles 7 and 8 of the CFREU, though it was finally signed by virtue of Articles 82(1)(d) and 87(2)(a) TFEU⁵⁵³; the EU-US PNR Agreement of 2012 was instead proposed by virtue of Article 82, 87 and 218(6)(a) TFEU and concluded accordingly⁵⁵⁴.

With *Opinion 1/15*, the CJEU clarified that PNR Agreements shall in future be based on Articles 16(2) and 87(2)(a) TFEU. The CJEU distanced itself from its previous judgment by highlighting that the situation post-Lisbon was different and that the ruling on the scope of the DPD should have not entailed any limitation to Article 16 TFEU. To assess on which legal bases the draft PNR Agreement should have been based, the CJEU looked at the purpose and contents of the measure⁵⁵⁵. Opting for a fragmented and an instrumental approach to the goals pursued by the envisaged agreement⁵⁵⁶, the CJEU maintained that the objective and content pursued by the draft Agreement was twofold: on one hand, it aimed at combating terrorism and serious transnational crime; on the other, it sought to safeguard an

⁵⁵⁰ Treaty establishing the European Community (Consolidated version 2002), *OJ C* 325, 24.12.2002, pp. 33-184.

⁵⁵¹ C-317/04 and C-318/04, *European Parliament v Council of the European Union and Commission of the European Communities*, para. 70. Remarkably, the following initiatives on PNR Agreements were based on Articles 95, 300(2) and 300(3) of the 1997 TEC as for the EU-Canada PNR Agreement of 2006. The EU-Australia PNR Agreement of 2008, instead, was promoted on the basis of Articles 24 and 38 of the 1997 TEU, and the same goes for the subsequent EU-US Agreement of 2006. See the comments made by: Marise Cremona, “External Relations of the EU and the Member States: Competences, Mixed Agreements, International Responsibility, and Effect of International Law”, *EUI Working Paper*, No. 22, 2006, pp. 1-40, p. 12, and Valsamis Mitsilegas, *EU Criminal Law*, Oxford, Hart Publishing, 2009, pp. 304-307.

⁵⁵² Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries, COM(2010) 0492 final, Brussels, 21.9.2010.

⁵⁵³ See the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, *OJ L* 186, 14.7.2012, pp. 4-16, and the Council Decision 2012/381/EU of 13 December 2011 on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, *OJ L* 186, 14.7.2012, p. 3.

⁵⁵⁴ See the Council Decision 2012/472/EU of 26 April 2012 on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, *OJ L* 215, 11.8.2012, p. 4, under revision according to “Les États membres soutiennent la poursuite des accords sur les données PNR avec l’Australie et les États-Unis”, *Bulletin Quotidien Europe*, No. 12722, 20.5.2021.

⁵⁵⁵ See Annegret Engel, *The Choice of Legal Basis for Acts of the European Union: Competence Overlaps, Institutional Preferences, and Legal Basis Litigation*, Cardiff, Springer, 2018.

⁵⁵⁶ Eleftheria Neframi, “Vertical Division of Competences and the Objectives of the European Union’s External Action”, in Marise Cremona and Anne Thies, *op. cit.*, pp. 73-94, p. 89.

adequate level of protection for the processing of personal data⁵⁵⁷. Specifically, the CJEU affirmed that Article 16 TFEU should certainly have been considered as the correct legal basis, since the protection of personal data was one of the essential aims or components of the agreement⁵⁵⁸. With regard to the AFSJ, Article 87(2)(a) TFEU was deemed to be appropriate even though ‘[...] data is initially collected by air carriers for commercial purposes and not by a competent authority in relation to the prevention, detection and investigation of criminal offences’⁵⁵⁹. Conversely, the CJEU discarded Article 82(1)(d) TFEU⁵⁶⁰ since no direct link could be established between this legal basis and Article 67(3) TFEU⁵⁶¹. All in all, as Articles 87(2)(a) and 16(2) TFEU required the adoption of measures under the ordinary legislative procedure, the draft Agreement should have been underpinned by both⁵⁶², which does not clarify whether the transfer of PNR by air carriers fall under scope of the GDPR or the LED. Should the CJEU embrace the position that Advocate General Pitruzzella has recently assumed⁵⁶³, then, the GDPR would be applicable to the processing activities as well as the transfer of personal data by air carriers to the national passenger information unit. Specifically, Pitruzzella highlights that the economic operator has the legal obligation to transfer personal data, but it ‘has not been entrusted with any prerogative of public authority’ within the meaning of Article 3(7)(b) of the LED⁵⁶⁴.

Opinion 1/15 puts under discussion the validity of other measures, such as the EU-US SWIFT Agreement. The EU-US SWIFT Agreement was based on Articles 87(2)(a), 88(2) and 218(6)(a) TFEU⁵⁶⁵ and was negotiated in the framework of the Terrorist Finance

⁵⁵⁷ *Opinion 1/15*, paras. 112-135 and our analysis in Chapter II.

⁵⁵⁸ *Ibid.*, para. 113 ff.

⁵⁵⁹ Opinion of Advocate General Mengozzi, *Opinion 1/15*, para. 101.

⁵⁶⁰ *Ibid.*, para. 108.

⁵⁶¹ According to it: ‘The Union shall endeavour to ensure a high level of security through measures to prevent and combat crime, racism and xenophobia, and through measures for coordination and cooperation between police and judicial authorities and other competent authorities, as well as through the mutual recognition of judgments in criminal matters and, if necessary, through the approximation of criminal laws’.

⁵⁶² The CJEU maintains that the ordinary legislative procedure is not compatible with the special legislative procedures that contemplate the unanimity in the Council, instead of the qualified majority. See, among others, C-300/89, *Commission of the European Communities v Council of the European Communities*, 11 June 1991, EU:C:1991:244.

⁵⁶³ Opinion of Advocate General Pitruzzella, C-817/19, *Ligue des droits humains v Conseil des ministres*, 27 January 2022, EU:C:2022:65, paras. 39-53. Conversely, the processing of personal data by passenger information units, national competent authorities, and the security and intelligence services of the Member State concerned would be covered by the PNR Directive only (paras. 54-59).

⁵⁶⁴ *Ibid.*, para. 44 (our own translation). In para. 60, Advocate General found that the same goes to the transfer of Advance Passenger Information (API) by carriers to the competent national authorities for improving border controls and combating illegal immigration, regulated under Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261, 6.8.2004, pp. 24-27 (API Directive hereinafter).

⁵⁶⁵ For an exhaustive analysis of the negotiation, re-negotiation, and conclusion of the SWIFT Agreement between the EU and the US see Juan Santos Vara, “La transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos”, *Cuadernos de la Cátedra de Seguridad Salmantina*, No. 7, 2012, pp. 1-

Tracking Program⁵⁶⁶ (TFTP), but already, by 2010, the EDPS was questioning the chosen legal basis, since the Agreement:

‘[...] does not envisage using Article 16 TFEU as a legal basis, despite the fact that Article 1.1 of the proposed agreement underlines a high level of data protection as one of its main purposes. In this regard, EDPS reiterates that such an Agreement not only relates to the exchange of personal data, but also to the protection of these data. Article 16 TFEU is therefore not less relevant as legal basis than Articles 82 and 87 TFEU relating to law enforcement cooperation that have been chosen as legal bases’⁵⁶⁷.

The Court had had not revised such an Agreement yet, to the displeasure of the European Parliament⁵⁶⁸, but if it would we can expect that it would support the Supervisor’s opinion. Indeed, *Opinion 1/15* represents a real turning point in the exercise of the EU competence based on Article 16(2) TFEU. With it, the CJEU makes the data protection disposition visible *vis-à-vis* PJCCM objectives, and it also gives another important interpretation regarding the EU’s competence on personal data: although Article 16(2) TFEU regulates both the EU competence on the protection of personal data and on the free movement of such data, it falls short of regulating the “flow of data” under sector-specific regulations that refer to concrete EU policies, at least as far as its external exercise is concerned⁵⁶⁹.

25, and Id., “El acuerdo SWIFT con Estados Unidos: génesis, alcance y consecuencias”, in José Martín y Pérez de Nanclares, *La dimensión exterior del espacio de libertad, seguridad y justicia de la Unión Europea*, Madrid, Iustel, 2012, pp. 355-380.

⁵⁶⁶ The TFTP was adopted under the Bush Administration as a response to the 11-S attacks and allowed US authorities to access EU citizens’ data gathered by the Society for the Worldwide Interbank Financial Telecommunication company since this, although being Belgian, kept some of its servers in the US territory. Once this mechanism had been unveiled, the Society for the Worldwide Interbank Financial Telecommunication company decided to move its servers to the EU territory so that the data processed under its responsibility would have been safeguarded under EU data protection standards. See the insight analysis conducted by the Opinion of the Article 29 DPWP No. 10/2006 on *the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, Brussels, 22.11.2006.

⁵⁶⁷ See the Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (TFTP II), *OJC* 355, 29.12.2010, pp. 10-15, para. 5. As Mara Wesseling, “An EU Terrorist Finance Tracking System”, *Royal United Services Institute for Defence and Security Studies*, 8.09.2016, available at rusi.org, underlines, the impact assessment conducted by the European Commission on this regard made the European Commission abandoning the submission of a formal proposal on a European TFTP because the necessity of its adoption was not well founded and because of its potential impacts on fundamental rights and additional costs.

⁵⁶⁸ See the European Parliament resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance (2013/2831(RSP)), *OJC* 208, 10.6.2016, pp. 153-156, and the European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens’ fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)), *OJC* 378, 9.11.2017, pp. 10-135. Among scholars, see Davor Jančić “The Role of the European Parliament and the US Congress in Shaping Transatlantic Relations: TTIP, NSA Surveillance, and CIA Renditions”, *Journal Common Market Studies*, Vol. 54, No. 4, 2016, pp. 896-912, and Katharina Meissner, “Democratizing EU External Relations: The European Parliament’s Informal Role in SWIFT, ACTA, and TTIP”, *European Foreign Affairs Review*, Vol. 21, No. 2, 2016, pp. 269-288.

⁵⁶⁹ See further Chapter II.

c) Aligning existing acts regarding the Law Enforcement Directive

The LED leaves Union acts that entered into force before 6 May 2016 in the fields of PJCCM that already regulate the processing of personal data between Member States and the access of designated authorities to information systems established pursuant to the Treaties within the scope of LED unaffected⁵⁷⁰. As a result, the criminal area is still a maze of instruments that requires close analysis of the legislative measures enforceable in the Member States for which the LED represents a framework instrument⁵⁷¹.

The LED required the European Commission to revise ‘[...] other legal acts adopted by the Union which regulate processing by the competent authorities for the purposes set out in Article 1(1) including those referred to in Article 60’ by 6 May 2019⁵⁷². The evaluation was published in the Communication of June 2020, where the European Commission found that sixteen instruments would not need to be amended⁵⁷³. Seven of them – including the European Arrest Warrant⁵⁷⁴ and the Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol⁵⁷⁵ – did not directly relate to any data protection issues, but the European Commission believed that the LED would be applicable to them as soon as it was transposed into the Member States’ legal orders⁵⁷⁶. Three other instruments – among which the European protection order⁵⁷⁷ that referred to the DPFD – needed to be amended so as to refer to the LED as of 6 May 2018. Similarly, the LED was found to be applicable to three existing international agreements concluded by the Member

⁵⁷⁰ Article 60 LED. A summary of the EU instruments in force in the criminal fields is available in Council of the EU, *European Union instruments in the field of criminal law and related texts*, Brussels, 2019, available at www.consilium.europa.eu.

⁵⁷¹ Recital (94) LED calls for the European Commission to evaluate the consistency between the one established in the Directive and the existing instruments so as to make appropriate proposals.

⁵⁷² Article 62(6) LED.

⁵⁷³ See the Communication from the Commission to the European Parliament and the Council, COM(2020) 262 final, Brussels, 24.6.2020. Cristina Blasi Casagran, *op. cit.*, pp. 48 ff., analyses some of these instruments dividing them between preventive measures that collect data for untargeted people – PNR, European Terrorist Finance Tracking System, the SIS, the VIS, the Eurodac, and the CIS – and as a response to criminal investigation for targeted individuals – Prüm Decision, the Swedish Initiative, the ECRIS, and European Investigative Order.

⁵⁷⁴ Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, *OJ L* 190, 18.7.2002, pp. 1-20.

⁵⁷⁵ Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with International Criminal Police Organization, *OJ L* 27, 29.1.2005, pp. 61-62.

⁵⁷⁶ Communication from the Commission to the European Parliament and the Council, COM(2020) 262 final, Brussels, 24.6.2020, pp. 2 and 3.

⁵⁷⁷ Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European protection order, *OJ L* 338, 21.12.2011, pp. 2-18.

States, as was the case of the Convention on Mutual Assistance in Criminal Matters⁵⁷⁸. The three instruments that were revised are:

- the VIS⁵⁷⁹, and the Dublin III Regulation⁵⁸⁰ in whose text and negotiations (respectively) the LED had already been taken into account, and
- the EU-US Mutual Legal Assistance Agreement in the light of the complementary EU-US Umbrella Agreement⁵⁸¹.

In addition, those instruments that remained unaffected by the LED or were not aligned with it, required the intervention of the co-legislators. The European Commission took into account ten such instruments⁵⁸²:

- the Council Framework Decision on Joint Investigation Teams⁵⁸³;
- the Council Decision on exchange of information and cooperation concerning terrorist offences⁵⁸⁴;
- the Swedish Initiative;
- the Council Decision on cooperation between Asset Recovery Offices⁵⁸⁵;
- the Prüm Decision;
- the CIS⁵⁸⁶;

⁵⁷⁸ Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention, *OJ C* 197, 12.7.2000, pp. 1-2.

⁵⁷⁹ Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA, COM(2018) 302 final, Brussels, 16.5.2018.

⁵⁸⁰ Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast), COM(2016) 0272 final, Brussels, 4.5.2016.

⁵⁸¹ Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, *OJ L* 336, 10.12.2016, pp. 3-13.

⁵⁸² Communication from the Commission to the European Parliament and the Council, COM(2020) 262 final, Brussels, 24.6.2020, p. 5 ff.

⁵⁸³ Council Framework Decision of 13 June 2002 on joint investigation teams, *OJ L* 162, 20.6.2002, pp. 1-3.

⁵⁸⁴ Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences, *OJ L* 253, 29.9.2005, pp. 22-24, and the Proposal for a Directive of the European Parliament and of the Council amending Council Decision 2005/671/JHA, as regards its alignment with Union rules on the protection of personal data, COM(2021) 767 final, Brussels, 1.12.2021.

⁵⁸⁵ Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime, *OJ L* 332, 18.12.2007, pp. 103-105.

⁵⁸⁶ Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes, *OJ L* 323, 10.12.2009, pp. 20-30.

- the Mutual Legal Assistance Agreement with Japan⁵⁸⁷;
- the European Investigative Order;
- the Directive on exchange of information on road safety-related traffic offences⁵⁸⁸, and
- the PNR Directive⁵⁸⁹.

The complexity and the variety of instruments in place, many of which have not yet been implemented by certain Member States that persist in a default position of non-compliance, makes these instruments ineffective, while spurring the use of unofficial channels to request and exchange the relevant information. As Prof. Blasi Casagran highlights:

‘None of the EU provisions on cross-borders policing precluded bilateral arrangements. Thus, these two countries did not use any channel for exchanging information, nor did they involve any EU agency such as Europol or Eurojust. This is even more problematic since crime-related information is not exchanged through secure channels, meaning it can also be easily intercepted and exposed’⁵⁹⁰.

Under the aegis of the new LED, the EU has a not-to-be-missed opportunity, that is, the chance to formalise, or even centralise, the channels through which Member States exchange information for PJCCM purposes⁵⁹¹. On 8 December 2021, the European Commission presented a new package⁵⁹², that together with the long-awaited revision of the Schengen Borders Code⁵⁹³, aims at establishing a Police Cooperation Code ‘with the objective of streamlining, enhancing, developing, modernising and facilitating law enforcement cooperation between relevant national agencies, thus supporting Member States in their fight

⁵⁸⁷ Agreement between the European Union and Japan on mutual legal assistance in criminal matters, *OJ L* 39, 12.2.2010, pp. 20-35.

⁵⁸⁸ Directive (EU) 2015/413 of the European Parliament and of the Council of 11 March 2015 facilitating cross-border exchange of information on road-safety-related traffic offences, *OJ L* 68, 13.3.2015, pp. 9-25.

⁵⁸⁹ Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, *OJ L* 119, 4.5.2016, pp. 132-149. However, as PNR Directive entered into force on the 15 May 2016 its dispositions shall be read in conjunction with the new LED anyway and, in case of contrast, the latter prevails.

⁵⁹⁰ Cristina Blasi Casagran, *op. cit.*, p. 22. The author takes as an example the France and Spain collaboration related to the investigations for the Euskadi Ta Askatasuna terrorist group.

⁵⁹¹ Recital (95) LED:

‘In order to ensure a comprehensive and consistent protection of personal data in the Union, international agreements which were concluded by Member States prior to the date of entry into force of this Directive and which comply with the relevant Union law applicable prior to that date should remain in force until amended, replaced or revoked’.

⁵⁹² “La Commission européenne propose de renforcer les outils de coopération policière dans l'UE”, *Bulletin Quotidien Europe*, No. 12849, 9.12.2021.

⁵⁹³ Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), *OJ L* 77, 23.3.2016, pp. 1-52 (Schengen Borders Code hereinafter).

against serious and organised crime and terrorism’⁵⁹⁴. The package is made up of three Proposals:

- a Proposal for a Council Recommendation on operational police cooperation⁵⁹⁵ directed at establishing ‘common standards to allow police officers to cooperate effectively with their colleagues in other Member States’ by virtue of Articles 87(3) and 89 of the TFEU, read in conjunction with Article 292 of the TFEU⁵⁹⁶;
- a Proposal for a Prüm II Regulation⁵⁹⁷ based on Articles 16, 87(2)(a), and 88(2) TFEU to ‘reinforce the exchange of information between Member States and therefore provide EU law enforcement authorities with enhanced tools to fight crime and terrorism [by] reinforcing and modernising the framework and allowing interoperability with other EU information systems’⁵⁹⁸, and
- a Proposal for a Directive to revise the Swedish Framework⁵⁹⁹ underpinned by Article 87(2)(a) TFEU that addresses three main concerns: first, the lack of clear and robust common rules on information exchange that should be overcome through the adoption of harmonised rules, including on the protection of personal data⁶⁰⁰; second, the lack of common structures and efficient management tools for exchanging information that call for a ‘modernisation’ of the Single Points of Contacts and the implementation, *inter alia*, of a Case Management System (CMS)⁶⁰¹ and, third, the lack of common practice in the use of existing communication channel(s) to exchange information within the EU which should result in the enhancement of

⁵⁹⁴ Proposal for a Directive of the European Parliament and of the Council on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA, COM(2021) 782 final, Brussels, 8.12.2021, pp. 2-3.

⁵⁹⁵ Proposal for a Council Recommendation on operational police cooperation, COM(2021) 780 final, Brussels, 8.12.2021.

⁵⁹⁶ *Ibid.*, p. 6.

⁵⁹⁷ Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation (“Prüm II”), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council, COM(2021)784 final, Brussels, 8.12.2021.

⁵⁹⁸ *Ibidem*.

⁵⁹⁹ Proposal for a Directive of the European Parliament and of the Council, COM(2021) 782 final, Brussels, 8.12.2021, pp. 2-3.

⁶⁰⁰ *Ibid.*, recitals (7) and (8) suggesting that, in any case, the data protection frameworks of the SIS, the Europol, the PNR Directive, the TFTP, and the Prüm framework as well as the European Commission’s Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, Strasbourg, 17.4.2018.

⁶⁰¹ It foresees that the Single Point of Contact would be made of: national law enforcement authorities; the Europol National Unit; the SIRENE Bureau; the Passenger Information Unit, and the Interpol National Central Bureau.

Europol's role as a 'criminal information hub' while ensuring the use of SIENA as the preferred communication channel⁶⁰².

Notably, the Proposal for a Council Recommendation on operational police cooperation seeks to align rules on surveillance, hot pursuit, joint patrols and other joint operations across national territories – e.g., with the support of the European Commission and Europol's coordination platform – and to deploy hot pursuit and joint patrols in intra-EU border areas to: combat migrant smuggling; prevent and detect illegal migrants who remain within a host country, to fight human trafficking and to identify and protect victims. During these operations, law enforcement authorities should be granted access to national, EU, and international databases via one of the four components implemented by the interoperability package, called ESP⁶⁰³. According to the European Commission, these measures should be accompanied by a revision of domestic rules and of bi- and multilateral agreements concluded with other Member States⁶⁰⁴.

In addition, the European Commission is proposing to implement two 'central routers'⁶⁰⁵ – the Prüm II router and the EPRIS – that would act as connecting points between Member States so as to:

- provide a technical solution for the efficient automated exchange of data between law enforcement authorities to make them aware of relevant data that is available in the national database of another Member State;
- ensure that more relevant data – such as facial images and police records, existing, stored data on DNA profiles, dactyloscopic data, and vehicle registration data – from national databases in other Member States is available to all competent law enforcement authorities;
- ensure that third country-sourced biometric data from Europol's databases can be automatically checked by Member States' law enforcement authorities, and *vice versa* as far as Member States' national databases are concerned, and

⁶⁰² Proposal for a Directive of the European Parliament and of the Council, COM(2021) 782 final, Brussels, 8.12.2021, pp. 2-3, p. 3 ff.

⁶⁰³ See further Chapter 5.

⁶⁰⁴ Proposal for a Council Recommendation, COM(2021) 780 final, Brussels, 8.12.2021, p. 15.

⁶⁰⁵ The European Commission finds it a mid-solution between a centralised and decentralised system provided that Member States would connect to these routers instead of each other's databases according to the Proposal for a Regulation of the European Parliament and of the Council, COM(2021)784 final, Brussels, 8.12.2021, p. 4: 'These routers would serve as message brokers forwarding search transactions and replies to national systems, without creating new data processes, enlarging access rights or replacing national databases'.

- provide law enforcement authorities with efficient access to the data corresponding to a ‘hit’ that is available in the national database of another Member State⁶⁰⁶.

Notably, the Proposal for a Directive to revise the Swedish Initiative is guided by three main principles: availability; equivalent access, and confidentiality⁶⁰⁷. According to the principle of availability, the information should be exchanged among the Single Point of Contacts and the law enforcement authorities, either spontaneously, or upon their request, making it possible for the law enforcement authorities of another Member State, other than the one requested it, to receive the information. The principle of equivalent access, instead, imposes on the Single Point of Contacts and law enforcement authorities of a Member State the duty of applying equivalent conditions for requesting and providing the information to the Single Point of Contacts and law enforcement authorities of another Member State. Finally, the principle of confidentiality imposes on the Single Point of Contacts and law enforcement authorities receiving the information the duty to respect the confidentiality requirements imposed by the providers of the information.

The three Proposals must be in line with the data protection framework established by the LED or, they might establish enhanced guarantees according to each specific system under the *lex specialis* formula.

3.2.2. Data protection as a split conferred competence: the impact of variable geometry on Article 16 of the Treaty on the Functioning of the European Union

The strong desire of the European Community to achieve an area of free movement within the Member States’ territories meant that its institutions had to accept that certain states maintained an intergovernmental position with regard to some of its policies that fall under the former JHA Area⁶⁰⁸. Specifically, when the Schengen *acquis*⁶⁰⁹ was integrated into the Amsterdam Treaty⁶¹⁰, the Community granted privileged regimes to the United Kingdom,

⁶⁰⁶ *Ibid.*, p. 2.

⁶⁰⁷ *Ibid.*, recital (9) and Article 3.

⁶⁰⁸ Recalling Steve Peers, *EU Justice and Home Affairs Law, IV Ed., Volume I: EU Immigration and Asylum Law*, Oxford, Oxford EU Law Library, 2016, p. 26, the resulting patchwork of legal frameworks was due to the ‘[...] reluctance of several ‘old’ member States to participate fully in EU integration in this area for various reasons, the unwillingness of all ‘old’ Member States to apply the full Schengen *acquis* immediately to new Member States, and the interest among several non-Member States in adopting the relevant EU measures’.

⁶⁰⁹ See the Council Decision of 20 May 1999 concerning the definition of the Schengen *acquis* for the purpose of determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the *acquis*, *OJ L* 176/1, 10.7.1999.

⁶¹⁰ In the occasion of the integration of the Schengen *acquis* into the Amsterdam Treaty, the TEC’s legal bases were adapted and/or modified. See the Council Decision 1999/435/EC of 20 May 1999 concerning the definition of the Schengen *acquis* for the purpose of determining, in conformity with the relevant provisions of

Ireland, and Denmark which gave birth to a complex interaction between these states and the other Members. In parallel, Schengen Associated Countries that are part of the European Travel Association on Schengen – namely Iceland, Lichtenstein, Norway, and Switzerland – had already adhered to the Convention implementing the Schengen Agreement and joined the EU institutional framework within the limits of the Schengen *acquis*⁶¹¹. All in all, measures adopted by the EU based on freedom, security and justice legal bases may, or may not, constitute a development of the Schengen *acquis* according to the Convention implementing the Schengen Agreement's scope.

With the Lisbon Treaty, Ireland, and Denmark – and previously the United Kingdom – inherited their peculiar positions within the AFSJ⁶¹². Their regimes were set forth under Protocols No 20 and No 21 for the United Kingdom and Ireland, and Protocol No 22⁶¹³ as

the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the *acquis*, *OJ L* 176, 10.7.1999, pp. 1-16, and the Council Decision 1999/436/EC of 20 May 1999 determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the Schengen *acquis*, *OJ L* 176, 10.7.1999, pp. 17-30.

⁶¹¹ Agreement on the European Economic Area - Final Act - Joint Declarations - Declarations by the Governments of the Member States of the Community and the EFTA States - Arrangements - Agreed Minutes - Declarations by one or several of the Contracting Parties of the Agreement on the European Economic Area, *OJ L* 1, 3.1.1994, pp. 3-522. The agreement celebrated by Norway and Iceland with the Schengen states was replaced by the treaties of 1999 that extended the Schengen area to Norway and Iceland in March 2001. Switzerland negotiated with the European Community and the Union its own associated agreement in 2004, that entered into force in 2008, while Lichtenstein's Protocol was agreed in 2006, and came into force in 2011. Note that the participation of these states in the Schengen *acquis* may have given rise to disputes when privileged regimes are granted to them on the basis of their different cultural heritage which has been recognised as lawful by the CJEU as for Directive (EU) 2017/853 of the European Parliament and of the Council of 17 May 2017 amending Council Directive 91/477/EEC on control of the acquisition and possession of weapons (Text with EEA relevance), *OJ L* 137, 24.5.2017, pp. 22-39, in C-482/17, *Czech Republic, v European Parliament and Council of the European Union*, 3 December 2019, EU:C:2019:1035, paras. 159-171.

⁶¹² On variable geometry see: Steve Peers, 2016, *EU Justice and Home Affairs Law, IV Ed., Volume I: EU Immigration and Asylum Law*, *op. cit.*, p. 26; Petr Dostál, "Changing European Union: The Schengen Agreement" in Tomáš Havlíček, Milan Jeřábek, and Jaroslav Dokoupil, *Borders in Central Europe After the Schengen Agreement*, Cham, Springer, 2017, pp. 15-35; Juan Santos Vara and Elaine Fahey, "Transatlantic relations and the operation of AFSJ flexibility", in Steven Blockmans, *Differentiated integration in the EU from the inside looking out*, Brussels, Centre for European Policy Studies, 2014, pp. 103-126; Paula García Andrade, "La geometría variable y la dimensión exterior del espacio de libertad, seguridad y justicia", in José Martín y Pérez de Nanclares, 2012, *op. cit.*, pp. 87-122; Elaine Fahey, "Swimming in a sea of law: Reflections on water borders, Irish(-British)-Euro Relations and opting-out and opting-in after the Treaty of Lisbon", *Common Market Law Review*, Vol. 47, No. 3, 2010, pp. 673-707; Maria Fletcher, "Schengen, the European Court of Justice and Variable geometry under the Lisbon Treaty: Balancing the UK's 'Ins' and 'Outs'", *The European Constitutional Law Review*, Vol. 5, No. 1, 2009, pp. 71-98; Jorrit Rijpma, "Case C-77/05, United Kingdom v. Council, Judgment of the Grand Chamber of 18 December 2007, not yet reported, and Case C-137/05, United Kingdom v. Council, Judgment of the Grand Chamber of 18 December 2007, not yet reported", *Common Market Law Review*, Vol. 45, No. 3, 2008, pp. 835-852, and Mariona Illamola Dausà, "Hacia una gestión integrada de las fronteras: El Código de Fronteras Schengen y el cruce de fronteras en la Unión Europea", *Revista CIDOB d'Afers Internacionals*, No. 15, 2008, pp. 7-103.

⁶¹³ See Protocol No 20 on the application of certain aspects of Article 26 of the Treaty on the Functioning of the European Union to the United Kingdom and to Ireland, *OJ C* 326, 26.10.2012, p. 293-294; Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, *OJ C* 202, 7.6.2016, pp. 295-297, and Protocol No 22 on the position of Denmark, *OJ C* 326, 26.10.2012, pp. 299-303.

far as Denmark is concerned. Both Protocols No 21 and No 22 foresee a specific provision directed at limiting the range of Article 16 TFEU measures regarding the regulation of data processing activities in the realm of police and criminal judicial cooperation measures. Therefore, the EU competence on the protection of personal data follows the paths of what Prof. Govaere defines as ‘split conferral’ to discern it from the ordinary attribution of ‘full competences’⁶¹⁴. In Govaere’s opinion, split conferral refers to the fact that ‘most but not all of the Member States confer the competence to the EU’. Despite the suppression of the Greek pillar structure, this solution has been kept by the Lisbon Treaty and it concerns, for example, the AFSJ. Prof. Govaere finds that the position of these countries may become problematic when a multi-purposes measure bypasses the boundaries of variable geometry⁶¹⁵. Specifically, the application of the doctrine on the choice of the correct legal basis may void provisions that require the exercise of opt-in/opt-out rights by those Member States or it may exclude their participation *tout court*⁶¹⁶. In this sense, the author points out that, for the time being, the CJEU has avoided coupling ‘full conferral’ with ‘split conferral’ legal bases.

This is also the case of Article 16 TFEU, that passed under the CJEU’s scrutiny only once, that is, in *Opinion 1/15*⁶¹⁷. On that occasion, and although the European Parliament would have accepted to underpin the draft EU-Canada PNR Agreement on Articles 16, 82(1)(d) and Article 87(2)(a) TFEU, Ireland and the Council opposed that the idea the merging of legal bases would have been incompatible with the voting procedure to be maintained under Protocols No 21 and No 22 to the Lisbon Treaty. The Council alleged that while these States would have participated in the adoption of measures stemming from Article 16 TFEU, they could have not voted on measures adopted under Articles 87(2)(a) and 82(1)(d) TFEU unless they exercised their opt-in right. Advocate General Mengozzi rejected this assumption by recalling that the participation of these Member States in the AFSJ could not be considered as part of the choice of the correct legal basis, yet he admitted that their different degrees of participation may have put into question the compatibility of

⁶¹⁴ Inge Govaere, “Full, Crippled, Split Conferral of Powers Post-Lisbon”, in Marise Cremona, 2018, *op. cit.*, pp. 223-266.

⁶¹⁵ For example, in the case of the Philippine Agreement the CJEU, despite acknowledging the existence of a specific clause on readmission of nationals, decided to frame it under the EU development cooperation with third countries, see C-658/11, *European Parliament v Council of the European Union*, 24 June 2014, EU:C:2014:2025.

⁶¹⁶ As it happened for Article 79 TFEU in C-377/12, *European Commission v Council of the European Union*, 11 June 2014, OJ C 282, 25.8.2014, p. 3, where the CJEU maintained that a readmission clause inserted in a multi-scope agreement in the frame of the development cooperation policy was not sufficiently detailed so as to justify the recourse to a split conferral basis – i.e., opt-out rights form the United Kingdom. See also C-656/11, *United Kingdom of Great Britain and Northern Ireland v Council of the European Union*, 27 February 2014, EU:C:2014:97, and C-89/18, *A v Udlændingeog Integrationsministeriet*, 10 July 2019, EU:C:2019:580.

⁶¹⁷ Advocate General Mengozzi, *Opinion 1/15*.

the legal bases at stake from a procedural perspective. However, he evaluates the participation of the Denmark, Ireland, and the United Kingdom differently, as we analyse below⁶¹⁸.

a) The position of Denmark

Being part of the Convention implementing the Schengen Agreement⁶¹⁹, Denmark decided not to take part in the Schengen legal bases integrated in the European Community primary Law in 1997. Protocol No 22 of the TFEU determines the position of Denmark with respect to the Schengen *acquis*⁶²⁰. This affects both the freedom as well as the security sections, with the unique exception of the determination of third countries whose nationals must be in possession of a visa when crossing the external borders of the Member States as this policy, according to Article 6 of Protocol No 22, entirely binds Denmark⁶²¹. Protocol No 22 stresses that:

‘In particular, acts of the Union in the field of police cooperation and judicial cooperation in criminal matters adopted before the entry into force of the Treaty of Lisbon which are amended shall continue to be binding upon and applicable to Denmark unchanged’.

According to this Protocol, within a period of six months Denmark can notify whether it wants to take part in a measure adopted as a development of the Schengen *acquis* and, if it does so, it commits to integrate it in its national law⁶²². This notification creates an obligation under public international law between Denmark and the other Member States participating in such measures that is sealed under an international agreement. Similarly, the willingness of Denmark to participate in the AFSJ is limited to the intergovernmental framework and the integration of the JHA Area in the European Community law operated by the Amsterdam Treaty provided Denmark with a specific position that still characterises its regime with regard to current Title V TFEU⁶²³. Provided that Denmark has not adhered to the opt-in/opt-out regime established for Ireland – and previously for the United Kingdom too – to date, its participation in EU acts of secondary law that institutionalise the agreements concluded

⁶¹⁸ *Ibid.*, paras. 124 ff.

⁶¹⁹ Agreement on the accession of the Kingdom of Denmark to the convention implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at the common borders signed at Schengen on 19 June 1990, *OJL* 239, 22.9.2000, pp. 97-105.

⁶²⁰ See Protocol No 22.

⁶²¹ Florian Trauner and Imke Kruse, “EC Visa Facilitation and Readmission Agreement”, *Centre of European Policies Studies*, No. 290, Brussels, 2008, pp. 1-40, p. 10.

⁶²² Note that Article 7 of the Protocol No 22, would enable Denmark to adopt the opt-in/opt-out regime currently in place for Ireland – and previously the United Kingdom.

⁶²³ See Article 2 of the Protocol No 22.

among the EU Member States – Denmark included – is (arguably)⁶²⁴ resolved with the ratification of international treaties through which Denmark integrates EU acts. Article 2a of Protocol No 22 establishes that:

‘Article 2 of this Protocol shall also apply in respect of those rules laid down on the basis of Article 16 of the Treaty on the Functioning of the European Union which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of that Treaty’.

This Article transposes Denmark’s privileged regime that exists within the AFSJ upon Article 16 TFEU, for example, it enabled Denmark to decide whether or not to integrate the LED in its legal order, which it did by way of notification on 9 November 2016⁶²⁵. The relationship between Article 2a and Article 1 of Protocol No 22 was analysed in *Opinion 1/15* by the High Court⁶²⁶ following Advocate General Mengozzi’s Opinion. The latter put into evidence how Denmark’s participation may have impacted the negotiations from a procedural perspective, recalling that Denmark would have not been bound by any international treaty concluded by the EU within the AFSJ, if it was adopted by virtue of Article 87 TFEU, or if a twofold legal basis underpinned by Articles 16(2) and 87 TFEU was chosen. Hence, Denmark should have been excluded from the voting procedure on the draft Agreement to avoid its joining a group of Member States opposed to the adoption of the act and, consequently, preventing them from reaching the necessary qualified majority of votes, even if Denmark would not be finally bound by it⁶²⁷. In Mengozzi’s view, Denmark’s participation was deemed to be ‘merely formal’ and could not be regarded as procedurally incompatible with the doctrine on the choice of the correct legal basis. What remains unclear is if Denmark must not participate in the final voting stage, and whether it shall be prevented from influencing the negotiations of a measure it finally does not incorporate, by virtue of the principle of sincere cooperation.

⁶²⁴ Paula García Andrade, 2012, *op. cit.*, p. 111 ff., questions the applicability of Article 218 TFEU and the principle of good faith when international agreements are concluded with between the EU and its own Member States.

⁶²⁵ See the Council of the EU, *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA 14208/16*, 14208/16, Brussels, 9 November 2016.

⁶²⁶ *Opinion 1/15*, paras. 114-118.

⁶²⁷ See also the Declaration No 48 concerning the Protocol on the position of Denmark, *OJ C* 202, 7.6.2016, p. 353, in which it committed to not use its voting right to prevent the adoption of the provisions that are not applicable to it.

b) The position of Ireland (and previously the United Kingdom one)

When the Schengen *acquis* was integrated into the Amsterdam Treaty, the European Community accepted that the Member States not participating in the Convention implementing the Schengen Agreement could maintain a special position after its institutionalisation. Specifically, Ireland and the United Kingdom were given the option to take part in some of the provisions of the *acquis*⁶²⁸ so that both states could decide *à la charte* the dispositions they would be bound by⁶²⁹. The two countries agreed to not take part in free movement projects and correlated policies, including the management of external borders⁶³⁰. On the contrary, they adhered to those dispositions that related to the PJCCM. Therefore, although the United Kingdom⁶³¹ and Ireland are considered as Schengen countries, their participation in it is distinct from that practiced by other states. This distinction is of paramount importance, Ireland – and, previously, the United Kingdom – is not free to opt-in/opt-out from the whole Schengen system as its participation is defined in the decision of the Council that agreed, unanimously, on the conditions under which the country was welcomed into the Schengen enhanced cooperation system. Even so, the participation of Ireland in measures adopted under the PJCCM is not mandatory as it was granted the possibility to opt-in within three months of its proposal⁶³². On the contrary, Ireland – and previously the United Kingdom – benefits from a full opt-out/opt-in regime regarding those measures that stem from the AFSJ and do not constitute a development of the Schengen

⁶²⁸ See Article 4 of the Protocol annexed to the Treaty on European Union and to the Treaty establishing the European Community – Protocol integrating the Schengen *acquis* into the framework of the European Union, *OJ C* 340, 10.11.1997, p. 93, now Article 4 of the Protocol No 19 to the Lisbon Treaty on the Schengen *acquis* integrated into the framework of the European Union, *OJ C* 326, 26.10.2012, pp. 290-292, that states that the United Kingdom and Ireland may seek to take part to all or some parts of the Schengen *acquis*.

⁶²⁹ See, respectively, the Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis*, *OJ L* 131, 1.6.2000, pp. 43-47, and the Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis*, *OJ L* 64, 7.3.2002, pp. 20-23.

⁶³⁰ This choice goes back to the existing travel arrangements in place between these two countries – a sort of “mini-Schengen” or Common Travel Area – as mentioned in Protocol No 20. We could affirm that these Member States had “a permanent provisional access” to the Schengen area, since they did not want to lift the controls at the internal borders with crucial impact on their participation to the large-scale IT systems analysed in Chapter 5.

⁶³¹ As for the United Kingdom, we cannot avoid mentioning the fact that it withdrew the EU as for the 1 February 2020. In accordance with the withdrawal agreement the United Kingdom will be disconnected from the EU systems by the 31 December 2020, unless the negotiations would provide otherwise. See Article 63(1)(e) of the Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community 2019/C 384 I/01, *XT/21054/2019/INIT*, *OJ C* 384I, 12.11.2019, pp. 1-177.

⁶³² And even after it according to Article 4 of the Protocol No 19.

acquis. In these domains Ireland does not participate in any new measure unless it agrees to⁶³³.

The Lisbon Treaty inserted the new Article 6a within the AFSJ framework, according to which:

‘The United Kingdom and Ireland shall not be bound by the rules laid down on the basis of Article 16 of the Treaty on the Functioning of the European Union which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of that Treaty where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16’.

In *Opinion 1/15*, the CJEU lost an important opportunity to interpret such a disposition. While embracing Advocate General Mengozzi’s Opinion, the CJEU noted that both the United Kingdom and Ireland had exercised their opt-in right with regard to the EU-Canada PNR draft Agreement and, as a consequence, their position would have not modified the voting rules within the Council in light of Protocol No 21⁶³⁴.

On closer inspection, Article 6a deserves at least two additional comments. First, although the provision refers to the whole Chapter 4 and Chapter 5 of Title V TFEU, the Protocol really only relates to the AFSJ’s measures that fall outside the Schengen *acquis* which, instead, is regulated by Protocol No 19. *Ergo*, in case of a measure adopted under the Schengen *acquis* twinned with Article 16 TFEU, Protocol No 19 requires Ireland – and

⁶³³ See Protocol No 21, that regulates Ireland’s participation in those measures that constitute a development of the AFSJ that are not part of the Schengen *acquis*. Of course, this distinction raises other issues related to the establishment of whether a measure constitutes or not a development of the Schengen *acquis*. According to the see the C-482/08, *United Kingdom of Great Britain and Northern Ireland v Council of the European Union*, 16 October 2010, EU:C:2010:631, paras. 64 and 65:

‘[...] the question whether a measure constitutes a development of the Schengen *acquis* is separate from that of the legal basis on which that development must be founded. Every European Union measure must be based on a provision of the Treaties which confers on the European Union institutions the power to adopt that measure. [...] According to the Court’s settled case-law, the choice of legal basis for a European Union measure must rest on objective factors which are amenable to judicial review, including in particular the aim and the content of the measure [...]’.

As a consequence, this subject shall be treated at different stages according to C-77/05, *United Kingdom of Great Britain and Northern Ireland v Council of the European Union*, 18 December 2007, EU:C:2007:803, para. 77:

‘[...] by analogy with what applies in relation to the choice of the legal basis of a Community act, it must be concluded that [...] the classification of a Community act as a proposal or initiative to build upon the Schengen *acquis* within the meaning of the first subparagraph of Article 5(1) of the Schengen Protocol must rest on objective factors which are amenable to judicial review, including in particular the aim and the content of the act [...]’.

This assumption shall be valid not only for the constitutional legal bases that are not directly associated with the Schengen *acquis* – like for example civil judicial cooperation – but also for those legal bases that constitute a hybrid solution between the Schengen *acquis* and the AFSJ – e.g., Article 79(1)(c) TFEU on illegal migration and irregular residence as we explain in Chapter V.

⁶³⁴ *Opinion 1/15*, para. 109, and Advocate General Mengozzi, *Opinion 1/15*, para. 110.

previously the United Kingdom – to exercise its opt-in/opt-out right accordingly. Second, the derogation from Article 16 TFEU is limited to those rules ‘governing the forms of judicial cooperation in criminal matters or police cooperation’ Ireland – and previously the United Kingdom – has not opted-in. By taking Advocate General’s position with regard to Denmark as an example, it seems to us that in case of a twofold legal basis made from Articles 16(2) and 87(2)(a) TFEU, that Ireland – and previously the United Kingdom – shall be allowed to participate in the negotiations and finally vote for the conclusion of the international agreement only if it promptly notifies its willingness to opt-in to the international agreement. Otherwise, it would not appear reasonable that Ireland should vote on a measure it potentially never opts-in to⁶³⁵. However, unlike in the case of Denmark, there is no Declaration annexed to the Lisbon Treaty that points in this direction, so this conjecture may be easily rebutted.

⁶³⁵ This was not the case of the United Kingdom that actively participated in the LED: see the Council of the EU, *Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, 7979/15, Brussels, 16 April 2015, and the *Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, 16497/12 ADD 2, Brussels, 7 December 2012.

CHAPTER II

THE EUROPEAN UNION'S EXTERNAL COMPETENCE ON PERSONAL DATA AND ITS TRANSFER TO THIRD COUNTRIES AND INTERNATIONAL ORGANISATIONS

Having analysed the attributes characterising the EU's competence on the protection of personal data and on the internal free movement of such data, along with its range and limits according to the founding Treaties and the CFREU, this second Chapter analyses the external actions of the EU based on Article 16 of the TFEU, that is to say, the existence and nature of an (implied) EU external competence based on that Article.

Given that the principle of conferral is the point of departure for the EU's external relations, the doctrine on implied external powers is based on the relevant internal shared competence – in this case Article 16(2) TFEU – that empowers the EU to conclude international agreements. However, in the external sphere, the exercise of conferred competences is modelled so as to consolidate successful partnerships¹. Specifically, the principles underpinning the supranational legal order, of which the EU is a founder², are directed at creating cooperative solutions with third parties, considering their different interests³, but without hampering the credibility of its human rights rhetoric through internal/external inconsistencies⁴. As Advocate General Mengozzi recalled in *Opinion I/15*:

‘[...] the Court should ensure that the proposed measures, even when they take the form of international agreements envisaged, reflect a fair balance between the legitimate desire to maintain public security and the equally fundamental right for everyone to be able to enjoy a high level of protection of his private life and his own data’⁵.

¹ Loïc Azoulay, “Structural Principles: Internal and External”, in Marise Cremona, *Structural Principles in EU External Relations Law*, Portland, Hart Publishing, 2020, pp. 31-46, p. 41, specifies that:

‘[...] the need for the emergence of particular types of structural principles arose in two specific contexts. One way was the admission that, despite the fact that they join exclusive external competence, Union institutions may be unable to act in particular situations. [...] The need for structural principles arose more pressing out of the realization that the approach adopted in the ERTA case establishing the absolute precedence of the Union's institutional framework in the conduct of external action within the ambit of EU law was no longer tenable’.

² Principles related to the exercise of the EU competence in the external layer includes the principles of conferral, subsidiarity, and proportionality by virtue of Article 5 of the TEU. Yet, other principles become relevant when it comes to analyse the exercise of EU external competences like the principle of sincere cooperation sets forth in Article 4(3) TEU and the one of institutional balance foreseen under Article 13(2) TEU.

³ For example, with regard to the rule of law principle, Ilaria Vianello, “The Rule of Law as a Relationship Principle”, in Marise Cremona, 2020, *op. cit.*, pp. 225-240, p. 226, affirms that: ‘[...] the restructuring of the relations between of the Union and those ‘outside’ its legal system; it requires redefining the actorness of the EU in its relations with its external partners as well as the actorness of the partners themselves’.

⁴ Gjovalin Macaj and Joachim A. Koops, “Inconvenient multilateralism: The challenges of the EU as a player in the United Nations Human Rights Council”, in Erik Wetzel, *The EU as a “Global Player” in Human Rights*, Oxon, Routledge, 2011, pp. 66-81, p. 78.

⁵ Advocate General Mengozzi, *Opinion I/15*, para. 8.

Such a discretionary margin includes other important limits established by international law that the EU and its Member States are subject to⁶. In its external activity, the EU is called on to ‘strictly observe’ and ‘uphold and promote’ its values and interests as well as to ‘consolidate’ and ‘support’ human rights while contributing to their protection and that of its citizens⁷. The ‘universality and indivisibility of human rights and fundamental freedoms’, together with the principles of the Charter of the UN and international law⁸, guide the EU’s external action⁹, and underpin its loyalty to multilateralism¹⁰, in a way that does not discourage a third party from concluding the envisaged agreement.

With relation to the EU competence on the protection of personal data, this set of rules and principles impose on the EU the duty to safeguard the high level of protection it pursues internally in the face of third countries and international organisations that do not have equivalent rules in their internal orders. The specific objectives pursued by the EU in the exercise of its competence based on Article 16(2) TFEU must be found in the EU secondary law its external (implied) competence takes its roots from¹¹. With regard to the regime on the transfer of personal data to third countries and international organisations, these principals are set forth in Chapter V of, respectively, the GDPR, the LED, and the EUDPR¹². Provided the latter is based on the provisions of the first two legislative texts and, in any case, that it serves

⁶ In case the negotiations with the Council of Europe will be successful, the ECHR should be added to this list as soon as the EU will access to the Council of Europe as we commented in the previous Chapter.

⁷ Article 3(5) TEU:

‘In its relations with the wider world, the Union shall uphold and promote its values and interests and contribute to the protection of its citizens. It shall contribute to peace, security, the sustainable development of the Earth, solidarity and mutual respect among peoples, free and fair trade, eradication of poverty and the protection of human rights, in particular the rights of the child, as well as to the strict observance and the development of international law, including respect for the principles of the United Nations Charter’.

See, for example, María del Carmen Muñoz Rodríguez, *Democracia y derechos humanos en la acción exterior de la Unión Europea*, Madrid, Reus, 2010, and María Mercedes Candela Soriano, *Los Derechos Humanos, la democracia y el estado de derecho en la acción exterior de la Unión Europea: Evolución, actores, Instrumentos y Ejecución*, Madrid, Dykinson, 2006.

⁸ See Article 21(1) and (2)(b) TEU with regard to the concrete objectives the EU shall pursue.

⁹ Article 21(1), first paragraph, TEU.

¹⁰ Article 21(1), second paragraph, and Advocate General Mengozzi, *Opinion I/15*, para. 8. The European Commission’s commitment in spreading worldwide continental data protection standards is done at the UN level, by concluding an additional Protocol based on Article 17 of the ICCPR, and at the European level by encouraging adherence to the Council of Europe’s Convention No 108 – see the Opinion of the Article 29 DPWP No. 04/2014 on *surveillance of electronic communications for intelligence and national security purposes*, Brussels, 10.04.2014.

¹¹ Marise Cremona, “A Reticent Court? Policy Objectives and the Court of Justice”, in Marise Cremona and Anne Thies, *op. cit.*, pp. 15-32, p. 19, classifies them as ‘specific legislative objectives as expressed in legal acts, normally in the Preamble’.

¹² For example, still referring to the DPD, Dan Jerker B Svantesson, “The regulation of cross-border data flows”, *International Data Privacy Law*, No. 1, Vol. 3, 2011, pp. 180-198, highlights the importance of the accountability of the data exporter in and after the ‘border control’ phase, that is, legal grounds for which personal data can be exported.

as a framework to set down specific provisions in each institution, body, office, and agency's regulations, our analysis of the existence and nature of an (implied) EU external competence is limited to the GDPR and the LED. Under these legal frameworks, the transfer of personal data to third countries and international organisations¹³ is a data processing activity¹⁴ the lawfulness¹⁵ of which complements the other provisions set forth in the GDPR and the LED. Thus, the transfer of personal data constitutes an interference with the individual's fundamental right to the protection of personal data – i.e., Article 8 of the CFREU – and therefore must respect the limits envisaged by Article 52(1) CFREU¹⁶. As Prof. Kuner points out, any transfer should undergo a three-step analysis:

- first, a legal basis for the transfer to be lawful;
- second, the use of one of the legal mechanisms set forth under the regime on the transfer of personal data, and
- third, the existence of another legal basis justifying the lawfulness of the processing prior to the transfer.

As the legality of the data processing activity was assessed in Chapter I, the following section focuses on the second step for which, we recall, the EU was a pioneer in the issuance of enforceable rules on the transfer of personal data¹⁷. The legal mechanisms through which public authorities are entitled to exchange personal data are as follows:

1. the adoption of adequacy decisions by the European Commission¹⁸;
2. the existence of appropriate safeguards¹⁹ and, specifically:

¹³ In the frame of international organisations, the Guidelines of the EDPB No. 2/2020 on *Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies: Version 2.0*, Brussels, 15.12.2020, p. 6 ff., admits within this notion '[...] any organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two countries'. It was discarded, instead, the proposal of the Austrian delegation that suggested to refer to 'organizations and its subordinate bodies [...] or any other body, which is set up by, or on the basis of, an agreement under international law between two or more subjects of international law (i.e. countries and international organisations)', for which Non-Governmental Organisations (NGOs) are also included. On this point, see the Council of the EU, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) -Proposals regarding Chapter V*, 10198/14, Brussels, 23 May 2014, p. 4.

¹⁴ See C-317/04 and C-318/04, *Parliament v Council of the European Union and Commission of the European Communities*, EU:C:2006:346, para. 56.

¹⁵ Christopher Kuner, "Article 44: General Principles for transfer", in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *op. cit.*, pp. 755-770.

¹⁶ See the Guidelines of the EDPB No. 2/2018 on *derogations of Article 49 under Regulation 2016/679*, Brussels, 25.05.2018, p. 3.

¹⁷ Rolf H. Weber, "Transborder data transfers: concepts, regulatory approaches and new legislative initiatives", *International Data Privacy Law*, Vol. 3, No. 2, 2013, pp. 117-130, pointing out that the transfer of personal data has always been regulated in domestic as well as in international law as a specific sector of data protection. As analysed by the CJEU in one of its first judgments, C-101/01, *Bodil Lindqvist v Åklagarkammaren i Jönköping*.

¹⁸ Article 45 GDPR.

¹⁹ Articles 46(2) GDPR, as well as Articles 36 and 37 LED.

- the conclusion of legally binding (and enforceable) instruments, or
 - the provision of administrative arrangements, subject to authorisation from the competent supervisory authority²⁰, and
3. the derogation clauses set forth in the EU data protection *acquis*, among which the pursuit of important matters of public interest stands out²¹.

As different rules for transferring personal data exist, the range of the EU external actions, in terms of both protection and transfer, changes depending on the legal instrument chosen: if an adequacy decision does not exist, the transfer of personal data based on the dispositions regulating an appropriate safeguard²², or for those taking place due to a derogation clause²³, must be supported by a level of protection equivalent to that of the Union.

This Chapter addresses the normative existence and nature of the EU's external competence²⁴ for which purpose the adoption of adequacy decisions and the conclusion of international agreements are analysed. Specifically, the conclusion of 'legally binding (and enforceable) instruments' is analysed as one of the two facets that allow for the exercise of the (implied) EU external competence based on Article 16(2) TFEU. Even if the continental regime on the transfer of personal data to third countries and international organisations has already gained the attention of scholars²⁵, an exhaustive analysis in light of the theory of implied external powers has not been carried out so far. We believe that these two tracks of research take into account the specificities that shape the EU competence on personal data in its external dimension. Our purpose here is to highlight how the EU supranational framework is the most conducive forum to develop a leading international regime of data governance.

1. Brief notes on the doctrine of implied external powers

The doctrine on implied external competences²⁶ was formulated by the CJEU through its existing judgment *Commission of the European Communities v Council of the European*

²⁰ Article 46(3) GDPR. There is no correspondent provision in the LED.

²¹ Article 49 GDPR and 38 LED.

²² Article 46(1) GDPR maintains that: 'In the absence of a [adequacy] decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available'.

²³ Article 49(1) GDPR: 'In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following condition'.

²⁴ Eleftheria Neframi, 2014, *loc. cit.*

²⁵ See *infra*.

²⁶ See: Diego Javier Liñán Noguera, 2020, "La acción de la Unión: las relaciones exteriores (I)", *loc. cit.*, and Id., "La acción de la Unión: las relaciones exteriores (II)" in Araceli Mangas Martín and Diego Javier Liñán Noguera,

*Communities*²⁷ (*AETR/ERTA* case) which revolved around the existence of an implied external competence based on an underlying internal objective, underpinned by a conferred competence, so long as the European Community's intervention was necessary for its achievement. From that moment on, the CJEU's jurisprudence has continued to develop its international doctrine on implied powers²⁸, adapting it to the supranational legal framework, with important repercussions on the exercise of the EU's external competences of a shared nature. Today, this doctrine continues to be applicable when ascertaining whether and to what extent the EU is empowered to act externally.

The Lisbon Treaty inserted a new provision establishing that: 'The Union shall have legal personality'²⁹. This *manifesto* norm does not confer to the EU a general empowerment to act however it will on the international scene³⁰. On the contrary, EU action shall always be justified in the light of the principle of conferral – i.e., an *ad hoc* legal basis that empowers the EU to intervene³¹. Specifically, two problems have to be faced when dealing with EU external action:

2020, *op. cit.*, on-line resource; Roberto Adam and Antonio Tizzano, *Lineamenti di Diritto dell'Unione Europea*, Torino, Giappichelli Editore, 2022, pp. 383-419; Giorgio Gaja and Adelina Adina, *Introduzione al Diritto dell'Unione europea*, Urbino, Editori Laterza, 2020, pp. 203-234, and Marise Cremona, "External Relations and External Competence of the European Union: The Emergence of an Integrated Policy", in Paul Craig and Gráinne de Búrca, *op. cit.*, pp. 217-268.

²⁷ C-22/70, *Commission of the European Communities v Council of the European Communities*.

²⁸ International Court of Justice (ICJ), Advisory Opinion, *Reparation for Injuries Suffered in the Service of the United Nations*, 1949, ICJ Rep. 174, recalled in C-8/55, *Fédération Charbonnière de Belgique v High Authority of the European Coal and Steel Community*, 16 July 1956, EU:C:1956:7, para. 304.

²⁹ Article 47 TEU – see previously Article 6 of the Treaty on the European Coal and Steel Community signed in Paris on 18 April 1951, entered into force on 23 July 1952 (TECSC), and Articles 210 and 211 of the TEEC, then Article 210 of the 1992 TEC, and Article 281 of the 1997 TEC. The latter set forth that: 'The Community has legal personality'. Today, Paula García Andrade, *La acción exterior de la Unión Europea en la materia migratoria: Un problema de reparto de competencias*, Valencia, Tirant Lo Blanch, 2015, pp. 73-75, highlights that Article 47 of the TEU does not resolve the doubts surrounding the EU capacity to act internationally. Nevertheless, the interpretation given by the CJEU analysed *infra*, as well as the existence of other provisions expressly empowering the EU to conclude international agreements are clearly directed in this way.

³⁰ Article 6 of the Vienna Convention on the Law of Treaties between States and International Organizations or between International Organizations signed in Vienna on 21 March 1986, not yet entered into force, rules that: 'The capacity of an international organization to conclude treaties is governed by the rules of that organization'. On the topic, see Diego Javier Liñán Noguerras, "La subjetividad jurídico-internacional de la Unión" in Araceli Mangas and Diego Javier Liñán Noguerras, 2020, *op. cit.*, on-line resource; José Antonio Pastor Ridruejo, *op. cit.*, p. 70 ff.; Sobrino Heredia, "La subjetividad internacional de las organizaciones internacionales", in Manuel Diez de Velasco, *Instituciones de Derecho Internacional Público*, Madrid, Tecnos, 2016, pp. 346-370; Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *International Law as Law of the European Union*, Leiden, Martinus Nijhoff Publishers, 2012, and Manuel Diez de Velasco Vallejo, *Las Organizaciones Internacionales*, Madrid, Tecnos, 2010, p. 64 ff.

³¹ See the Declaration No 24 concerning the legal personality of the European Union, OJ C 326, 26.10.2012, p. 348: 'The Conference confirms that the fact that the European Union has a legal personality will not in any way authorise the Union to legislate or to act beyond the competences conferred upon it by the Member States in the Treaties'. Such a recognition overcomes the double identity issues stemming from the compresence of the European Community and the EU for the conclusion of horizontal mixed agreements to which we refer *infra*.

the existence of the competence, and its nature³². Both steps were added to the founding Treaties through Article 216(1) TFEU³³ and Article 3(2) TFEU³⁴ that brought with them all the ambiguities of the complex discourse on the existence and the nature of implied external competences.

1.1. The existence of implied European Union's external competences

As far as the existence of implied EU external competence is concerned – express external competences apart – in the *AETR/ERTA* case the CJEU advanced the idea that the (then) European Community could conclude international agreements when no express provision was foreseen by the Treaties³⁵. Specifically, the CJEU³⁶ recognised the “necessity” of EU external action to achieve one of the objectives referred to in the Treaties, that is, the establishment of a common policy on transport³⁷.

Following a literal interpretation of Article 216(1) TFEU, Prof. De Baere³⁸ maintains that the EU could derive its external competence when its need is foreseen in a legally binding

³² Paula García Andrade, 2015, *op. cit.*, p. 88 ff. The author recalls that Alan Dashwood and Joni Helikoski, *The General Law of E.C. External Relations*, London, Sweet/Maxwell, 2000, pp. 115-138, instead, proposed to determine the range of the EU internal competence and, second, evaluate whether the external action contribute to the achievement of such an objective.

³³ According to Article 216(1) TFEU: ‘The Union may conclude an agreement with one or more third countries or international organisations where the Treaties so provide or where the conclusion of an agreement is necessary in order to achieve, within the framework of the Union's policies, one of the objectives referred to in the Treaties, or is provided for in a legally binding Union act or is likely to affect common rules or alter their scope’.

³⁴ According to Article 3(2) TFEU: ‘The Union shall also have exclusive competence for the conclusion of an international agreement when its conclusion is provided for in a legislative act of the Union or is necessary to enable the Union to exercise its internal competence, or in so far as its conclusion may affect common rules or alter their scope’.

³⁵ Afterwards, see C-281, 283, 284, 285 and 287/85, *Germany and Others v Commission*, 9 July 1987, EU:C:1987:351. In this judgment, the Court annulled Commission Decision 85/410/EEC of 12 July 1985 relating to a proceeding under Article 85 of the TEEC (IV/4.204 Velcro/Aplix) (Only the French text is authentic), *OJ L* 233, 30.8.1985, pp. 22-32, establishing a prior notification procedure to inform on socio-cultural measures adopted by the Member States and aimed at the integration of foreign workers and members of their families. The notification could lead to a consultation procedure between the European Commission and the Member States which, by adopting common positions, would promote the rapprochement of State's migration policies.

³⁶ As it was confirmed in C-3, 4 and 6/76, *Cornelis Kramer and others*, 14 July 1976, EU:C:1976:114. The object of the controversy pivoted around the Dutch law establishing a top-up quota of fishing for the 1975 period of sole and plaices in the North-West Atlantic Sea and the consequent prohibition of fishing activities to specific types of vessels in the coast zone circumscribed in a twelve miles distance. The CJEU was called upon to assess the compatibility of the regime set forth by The Netherlands by virtue of the Convention on Future Multilateral Cooperation in Northeast Atlantic Fisheries, *U.N.T.S.* No. 1799, Vol. 157, p. 369, signed in Ottawa on 24 October 1978, entered into force on 1 January 1979 with the communitarian *acquis*.

³⁷ C-22/70, *Commission of the European Communities v Council of the European Communities*, p. 269:

‘This interpretation of Article 75 (1) of the Treaty is in accordance with common sense, with the ratio legis and with the principle that provisions should be given their full effect. It would have been unreasonable to provide for a common policy in a field as extensive as transport without conferring on the Community the means of taking appropriate action in respect of external relations, particularly since transport by its very nature frequently involves an international aspect transcending the framework of the Community alone’.

³⁸ See Article 4(4) TFEU and Geert De Baere, 2008, *op. cit.*, p. 68.

Union act, i.e., EU secondary law, instead of the founding Treaties³⁹. Prof. García Andrade firmly opposes such an idea by virtue of the paramount principle of conferral⁴⁰ that obliges the EU to act ‘within the framework of the Union-s policies’. In her words: ‘The Union shall therefore have competence to act externally when it has been given internal competence to attain a specific objective and its external action is necessary to attain that objective by the founding Treaties’⁴¹. Thus, the author clarifies that despite its fuzzy formulation, the principle of the affectation of common norms set forth in Article 216 TFEU *in fine* – i.e., that they ‘affect common rules or alter their scope’ – cannot become a source that affirms the existence of EU external competences⁴².

In the subsequent *Opinion 1/76*, the CJEU added that the EU is empowered externally not only when the EU exercises its competences while pursuing a common policy objective, but also when no measure has been previously deployed and the EU’s action is necessary to achieve one of the objectives internally assigned to it by a ‘Union policy’⁴³, notwithstanding whether it

³⁹ See Geert De Baere, “EU external action”, in Catherine Bernard and Steve Peers, *European Union Law*, Oxford, Oxford University Press, 2017, pp. 710-760, pp. 722-723, and Id., “Subsidiarity as a Structural Principle”, in Marise Cremona, 2018, *op. cit.*, pp. 92-116, p. 103. In reality, the author compares the wording used under Articles 216(1) TFEU – ‘legally binding Union act’ – with the one used in Article 3(2) TFEU – ‘legislative act of the Union’ – in order to distinguish the former as a source of attribution of competence, and the latter as a norm determining the exclusive nature of the EU external action. He observes that, in the end, the nature of the external competence depends on the law-making procedure by which the internal act granting that competence was adopted.

⁴⁰ Paula García Andrade, 2015, *op. cit.*, p. 96, recalling Article 5(2) TEU: ‘Under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States’. See also *Opinion 1/76*, 26 April 1977, EU:C:1977:63, para. 3, on the draft agreement establishing a European laying-up fund for inland waterway vessels, and *Opinion 2/94*, para. 26, where the CJEU had to assess whether the Community could have acceded the ECHR or not. Similarly, Alan Dashwood, Michael Dougan, Barry Rodger, Eleanor Spaventa, and Derrick Wyatt, *Wyatt and Dashwood’s European Union Law*, Oregon, Hart Publishing, 2011, p. 920, while referring to *Opinion 1/94*, 15 November 1994, EU:C:1994:384, para. 33, maintain that ‘[...] the significance of this instance of implied competence appears to have been misunderstood by those who saw fit to mention it in Article 216(1), owing to a failure to relate the statement cited above to its content in *Opinion 1/94*’.

⁴¹ *Ibid.*, p. 86 (the translation is ours).

⁴² For their part, Alan Dashwood, Michael Dougan, Barry Rodger, Eleanor Spaventa, and Derrick Wyatt, *op. cit.*, p. 921, recognise that such an expression refers to the *ERTA* judgment ‘[...] in its function as a source of competence for the Union to enter into international agreements where express conferral is lacking [...] Nevertheless, the enshrinement of the AETR principle in Article 216(1) appears wise, since its ‘existence function’ is logically inseparable from its ‘exclusivity function’, and not to have acknowledged the former might have given rise to uncertainty’.

⁴³ *Opinion 1/76*, on draft Agreement establishing a European laying-up fund for inland waterway vessels. *Ibid.*, para. 4:

‘This is particularly so in all cases in which internal power has already been used in order to adopt measures which come within the attainment of common policies. It is, however, not limited to that eventuality. Although the internal community measures are only adopted when the international agreement is concluded and made enforceable, as is envisaged in the present case by the proposal for a regulation to be submitted to the Council by the Commission, the power to bind the community vis-à-vis third countries nevertheless flows by implication from the provisions of the treaty creating the internal power and in so far as the participation of the community in the international agreement is, as here, necessary for the attainment of one of the objectives of the community’.

is a common one. Nevertheless, what constitutes ‘necessary’ actions is presented differently in the two rulings: while in the *AETR/ERTA* doctrine the CJEU widely interpreted it in the light of the paramount principle of the *effet utile*, in *Opinion 1/76*, the “necessity” of the EU intervention is narrowly elaborated ‘[...] so that the conclusion of the international agreement is necessary to achieve the objectives of the Treaty that cannot be achieved through the establishment of autonomous rules [...]’⁴⁴. Hence, given the lack of internal rules, the EU action must be the only way to achieve the objective pursued⁴⁵.

1.2. The nature of implied European Union’s external competences

When referring to the “affectation” criterion, Article 216(1) TFEU is really pointing out how the *AETR/ERTA* jurisprudence may turn internal shared competences into external exclusive ones, rather than shared or parallel ones. Leaving aside express external competences ‘by nature’, that must be inferred by each specific provision, Prof. García Andrade divides implied EU external competences into exclusive and non-exclusive: exclusivity is triggered by the *AETR/ERTA* direct and indirect effect – the author refers to the latter as ‘exclusivity by exercise’ as it represents the manifestation of the exercise of shared external competence for which the EU occupies the ‘external territory’ before the internal one – depending on whether the EU has already legislated on the matter internally or not; otherwise, ‘competences may be shared – in the absence of other exclusivity grounds, the Union is able to exercise them alone, with future pre-emption effects over Member States’ powers or parallel – in which the respective Union’s and Member States’ treaty making powers co-exist without the former having pre-emption effects on the latter’⁴⁶.

⁴⁴ *Opinion 1/76*, para. 115, where the conclusion of the international agreement on river navigation was the only way to involve Switzerland. In this way, and in the absence of a common policy, the exercise of implicit external competence of the EU is subsidiary to the exercise of internal competence ‘[...] only if the exercise of internal power does not allow the achievement of the objective pursued, will Union to exercise its implicit external competence’ by Paula García Andrade, 2015, *op. cit.*, p. 88.

⁴⁵ Also, in C-471/98, *Commission of the European Communities v Kingdom of Belgium*, 5 November 2002, EU:C:2002:628, the CJEU confirmed that in the field of air transport, for instance, the EU action would be hardly affective being this subject intrinsically international. Consequently, in numerous occasions ‘[...] it was found necessary to prescribe, through Community measures on air and sea transport, the treatment to be accorded to third-country carriers and to conclude corresponding agreements’, para. 72.

⁴⁶ Paula García Andrade, “EU external competences in the field of migration: how to act externally when thinking internally”, *Common Market Law Review*, No. 55, pp. 157-200, 2018, p. 165.

1.2.1. Implied external exclusive competences

a) The *AETR/ERTA* direct effect

When exclusivity in the external sphere arises from the exercise of internal competences – that is, when Member States count on EU internal legislation – the EU external competence is labelled as an ‘*AETR/ERTA* exclusivity’ since in the homonymous case-law the CJEU affirmed that implicitly alleged external competences should be considered exclusive due to the exercise of internal powers⁴⁷. Recalling the CJEU’s statement:

‘[...] every time that the Community, in order to apply a common policy provided for in the Treaty, adopts provisions that establish common standards, in whatever form, the Member States no longer have the power to either act individually or even collectively to contract obligations with third States that affect said norms’⁴⁸.

As a result, the principle of pre-emption turns the competences that are shared internally into exclusive ones when the EU adopts common rules in the application of a common policy⁴⁹. Nevertheless, in *AETR/ERTA*, the CJEU did not draw a perfect parallel between internal and external competences, as it specified that such an exclusivity stems from the principle of pre-emption – i.e., the occupation of the corresponding domain that is regulated internally. Therefore, the exclusivity of the EU competence should have been assessed on the basis of the real territory occupied and not as if the whole common policy was at stake. The following case law added further nuances to this principle.

- In *Opinion 1/91*, the CJEU specified that the exclusive or non-exclusive nature of the Community’s competence – not only common policies⁵⁰ – depended on the: ‘[...] scope of the measures which have been adopted by the Community institutions for the application of those provisions and which are of such kind as to deprive the Member

⁴⁷ *Ibid.*, p. 152, speaks about exclusivity *a priori* to evidence that the exercise of external competences is exclusive even before it is exercised. Specifically, the author points out a twofold reason: differently from internal competences whose exclusivity derives from the exercise of the correspondent competence, the external implied one is *ab origine* exclusive, and it defends a common interest underlying for the persecution of the integrity of the internal *acquis*. Hence, Member States are always prevented from acting notwithstanding the fact that norms agreed in the treaty contravene EU secondary law or not.

⁴⁸ C-22/70, *Commission of the European Communities v Council of the European Communities*, para. 17.

⁴⁹ Alan Dashwood, Michael Dougan, Barry Rodger, Eleanor Spaventa, and Derrick Wyatt, *op. cit.*, p. 914, underline the principle of primacy of EU law that makes the latter prevailing over Member States’ ones in case of conflict – see C-26/62, *Van Gend en Loos v Administratie der Belastingen*, 5 February 1963, EU:C:1963:1.

⁵⁰ C-3, 4 and 6/76, *Cornelis Kramer and others*, paras. 21-25. All in all, and although the European Community’s external action was strictly justified for the pursuit of an internal objective satisfying a common policy, in its following *Opinion 2/91*, para. 11, the CJEU also added that the *AETR/ERTA* doctrine is applicable to other dispositions of harmonisation adopted within domains other than EU common policies. This is reflected in Article 216 TFEU that clearly refers only to ‘policy’ and not to common policies.

States of an area of competence which they were able to exercise previously on a transitional basis [...]’⁵¹. Thus, the adoption of common norms prevents Member States from acting when the international agreement to be concluded can affect or alter the scope of the internal dispositions previously adopted⁵², which happens in cases where complete harmonisation is achieved internally⁵³ or whenever the internal legislation covers it to a large extent⁵⁴.

- In *Opinion 2/91*, the CJEU recalled that the exclusive character of the EU’s competence would have excluded the participation of the Member States, both internally and externally⁵⁵, and it also underlined that such exclusiveness derived from the range of the measures adopted internally. Therefore, regardless of the instrument adopted internally – be it a regulation, a directive, or a decision – it is the provision that, as soon as it binds the Member States, shall be considered as a ‘common rule’ and that may trigger the *AETR/ERTA* doctrine⁵⁶. In other words, “common standard” relates to all the EU norms binding the Member States without prejudice to the underlying approximation, harmonisation, or integration effect on Member States’ legal orders. However, the CJEU advanced that the choice of the legal basis is a symptom of the exclusiveness of the EU external competence, provided that it expressly opts for a certain degree of approximation.

⁵¹ *Opinion 1/91*, 14 December 1991, EU:C:1991:490, para. 9

⁵² In its subsequent *Opinion 1/92*, 10 April 1992, EU:C:1992:189, the CJEU was called to assess the compatibility of the new European Free Trade Association Court (EFTA Court) with the TEEC. The CJEU observed that the EFTA Court would have had jurisdiction only within the framework of EFTA and may be adhered to for: interpret the agreement or settle disputes between the contracting parties. Provided that in the frame of the latter proceeding, the CJEU may have been adhered to interpret the relevant rules, the CJEU ruled that the agreement should have been considered compatible as long as the decisions of the Joint Committee would have not affected the case-law of the CJEU and found that the EFTA Surveillance Authority and the Commission of the European Communities could have shared responsibility in the field of competition.

⁵³ C-22/70, *Commission of the European Communities v Council of the European Communities*, paras. 95 and 96. In the same line see C-471/98, *Commission of the European Communities v Kingdom of Belgium*.

⁵⁴ The CJEU has then clarified that the ‘sector’ may be made of different instruments and not a unique measure, for example in C-114/12, *European Parliament v Council of the European Union*, 4 September 2014, EU:C:2014:2151, para. 83. Here, the CJEU annulled the Council Decision authorising both the European Commission and the Member States to participate in the negotiations of the Convention of the Council of Europe on the protection of neighbouring rights of broadcasting organisation, *ETS* No. 34, signed in Strasbourg on 22 June 1960, entered into force on 1 July 1961, since the domain covered by it had been regulated by the EU ‘to a large extent’, which conferred it and exclusive competence by virtue of Article 3(2) TEU. However, as Prof. De Baere, 2008, *op. cit.*, p. 50, underlines, the CJEU has not given any indication yet on the moment in which it is understandable that the area has been ‘largely covered’.

⁵⁵ *Opinion 2/91*, 19 March 1993, EU:C:1993:106, para. 8.

⁵⁶ Paula García Andrade, 2015, *op. cit.*, p. 156. ‘If a provision of a regulation does not impose an obligation on the Member States, but merely empowers them to act in some way, it cannot be considered a “common rule” within the meaning of ERTA’ case law’ (our own translation).

- In *Opinion I/94*, the CJEU was called to assess the EU's capacity in participating in the General Agreement on Tariffs and Services (GATS) and the Agreement on Trade Related Intellectual Property Rights (TRIPS) created through the World Trade Organisation (WTO) and affirmed that only the Agreement on Technical Barriers to Trade fell entirely within the scope of the CCP for which purpose the (then) European Community had acquired exclusive competence according to Article 113 of the 1992 TEC, and that: '[...] Only in so far as common rules have been established at internal level does the external competence of the Community become exclusive. However, not all transport matters are already covered by common rules'⁵⁷.
- In *Opinion I/03*⁵⁸, the CJEU stated that the *AETR/ERTA* affectation criteria shall be cumulatively evaluated on the basis of a detailed analysis on the range, nature, and scope of application of the norms at stake, comparing the international instrument with the relevant EU legislation. Yet, a perfect overlap is not necessary, nor shall the commitments made be contradictory to EU rules⁵⁹: it suffices to say that the domain covered by the agreement has been largely covered by EU law. In addition, the CJEU recalled that how the relevant EU law might evolve, to the extent that is foreseeable at the time of the Member States' action, should be considered when determining the exclusiveness of the EU external action⁶⁰ by virtue of the principle of loyal cooperation enshrined in Article 4(3) TEU⁶¹.

⁵⁷ *Opinion I/94*, para. 77.

⁵⁸ *Opinion I/03*, 7 February 2006, EU:C:2006:81.

⁵⁹ *Opinion I/13*, 14 October 2014, EU:C:2014:2303, para. 86, where the Council of the EU, supported by other governments, alleged that the possibility that the EU exclusive external competence stems from the fact that the internal legislations has covered a specific domain to a large extent had not been codified under Article 3(2) TFEU.

⁶⁰ *Opinion I/03*, para. 126. Recalling that in the application of the *AETR/ERTA* doctrine the CJEU found that the regime established under Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, *OJ L 12*, 16.1.2001, pp. 1-23, would be affected by any agreement establishing an own global regime on norms of conflict similar to the one elaborated under EU law, and so did the Lugano Convention – see paras. 151-161.

⁶¹ Marise Cremona, "Structural Principles and their Role in EU External Relations Law", in Marise Cremona, 2020, *op. cit.*, pp. 3-30, p. 21, highlights that the principle of sincere cooperation acquires different shapes depending on whether it applies to exclusive or shared competences:

'In case of exclusive competence, the Member States may act only through joint or collective action. In case of shared competence the duty of cooperation is more flexible; it can involve an obligation not to obstruct the EU if an international initiative such as the negotiation of an agreement is underway; it can involve an obligation to act jointly with the EU institutions in particular circumstances [...] This proposition can come under strain: Commission v Sweden demonstrates a strong reading of the duty of cooperation in the case of a mixed agreement, and while it can be defended it comes perilously close to a denial of Member States competence to act at all'.

b) The reverse *AETR/ERTA* effect

The application of the principle of pre-emption in the exercise of external shared competences turns them into exclusive ones given their exercise – i.e., so-called ‘exclusivity by exercise’⁶². The foundation of this type of exclusiveness is regulated under Article 2(2) TFEU that establishes that Member States might exercise their powers to the extent that the EU has not done so, i.e., under the pre-emption principle⁶³.

As Prof. García Andrade underlines, in *Opinion 1/76* the CJEU did not maintain that the EU implied external power was automatically exclusive, as it was still focusing on the possibility that the EEC could act externally, rather than on the nature of its intervention. Instead, in its subsequent jurisprudence, the CJEU clarified that, in the absence of internal legislation, the EU competence to act externally is shared with the one of the Member States⁶⁴. In this sense, Member States can exercise their treaty-making power on the sidelines of the community *acquis* until the EU has not acted externally. In other words, the EU shall exercise its (implied) external⁶⁵ powers to acquire exclusivity in the international scene. Until that point, the EU external competence was shared with the one of the Member States, but this competence does not materialise until it occupies the ground externally⁶⁶.

This logic follows the so-called “reverse *AETR/ERTA* effect”, an expression used to point out that while concluding an international agreement, the EU also legislates internally so as to justify its empowerment as soon as it ratifies the treaty⁶⁷. Consequently, the “occupation” of

⁶² According to Paula García Andrade, 2015, *op. cit.*, p. 167: ‘While ERTA case law focuses on the effects that an internal occupation has at the external level, without the external competence having been previously exercised - it could therefore be described as “*a priori* exclusivity” - an “exclusivity by external exercise” would, as its name suggests, derive from the effects of the exercise of the external competence itself’ (our own translation).

⁶³ However, *ibid.*, pp. 171 and 172, underlines that still there are some conflicts on the possibility that this exclusivity too can be perceived as ‘*a priori*’.

⁶⁴ *Opinion 1/94*, para. 85, and *Opinion 2/92*, para. 32.

⁶⁵ This assumption is valid for both express and implied shared external competences, yet for the purpose of the current research the latter only is relevant.

⁶⁶ Thus, the situation could be assimilated to the one analysed *infra* in case of non-exclusive external competence, but differently from that situation the exclusivity by exercise only happens when the EU has not legislated internally. In this sense, see Paula García Andrade, 2015, *op. cit.*, p. 169 ff.: the author starts talking about external implied shared competences and terminates classifying the EU competence on readmission agreements by virtue of Article 79(3) TFEU as exclusive by exercise meaning that:

‘[...] at present, the exercise of this explicit concurrent competence by the Union will only have to justify that the requirements of the subsidiarity principle are fulfilled, and, once exercised, the field will be occupied by the Union with regard to that country, meaning that no new bilateral readmission agreements may be concluded between Member States and that same third country, except for the signature of implementing protocols of EU readmission agreements’.

⁶⁷ Merijn Chamon, “Provisional Application’s Novel Rationale: Facilitating Mixity in the EU’s Treaty Practice”, in Wybe Th. Douma, *The Evolving Nature of EU External Relations Law*, Berlin-Heidelberg, Springer, pp. 131-163, p. 148, and the relevant scholars cited therein.

the Member States' territory is not attributed (or not only) to the EU's external action, but also to the internal norms that derive from the incorporation of the international agreement into the supranational legal order. Actions by the Member States are pre-empted when they may affect or alter the scope of common norms, but in the absence of internal rules, the affectation shall be assessed *vis-à-vis* the agreement and its transposition in the common *acquis*⁶⁸.

To be precise, it is the exercise of external shared competences that differentiates this type of exclusiveness from the *AETR/ERTA* exclusivity analysed *supra*. Indeed, given the lack of internal dispositions, the paramount principle of subsidiarity⁶⁹ emerges to highlight the fact that the EU's external action shall always be justified in terms of the added value brought by the EU intervention to the singular activity undertaken by the Member States⁷⁰. In this regard, Prof. García Andrade recalls that if all twenty-seven Member States maintain a clear position toward a third country in crafting an international agreement, the common regulation that they want to achieve shows that the principle of subsidiarity is satisfied, and the EU shall act in their place. Otherwise, Member States would be infringing the Treaties' provisions, specifically the proceedings envisaged under Article 218 TFEU⁷¹. Besides, the principles of necessity and proportionality shall be duly justified in a way not very different from the exercise of shared internal competences⁷², but in a more effective manner than the exercise of explicit powers. As Prof. García Andrade notes:

‘This leads to a differentiation between the exercise of explicit and implied external powers. The former can be exercised by the Union once the subsidiarity principle is complied with. For the latter, the doctrine of Opinion 1/76 requires the Union to additionally justify that the conclusion of an international agreement is indispensable to

⁶⁸ Paula García Andrade, 2015, *op. cit.*, p. 173. This is the reason why, Prof. García Andrade speaks of a direct application of the pre-emption principle at the external level which is actually a good inspection. What she could have further stressed is the following reasoning: it is not the EU external action what really prevents the Member States to exercise their treaty making powers, but the effects the adoption of the correspondent common rules would have on it. In other words, the affectation is directed to internal and external norms as well, as they coincide when the EU legislates through its external competence.

⁶⁹ Jörg Monar, *The External Dimension of the EU's Area of Freedom, Security and Justice: Progress, potential and limitations after the Treaty of Lisbon*, Swedish Institute for European Policy Studies, 2012, p. 25: ‘Far from being a theoretical issue the Member States have repeatedly underlined this restriction on the expansion of EU action’. As far as the AFSJ is concerned, the author underlines that before the insertion of new sharing competences: ‘In each case, however, the use of a potential new legal competence will depend on the Member States willingness to exploit it and their perception of its potential to provide substantial “added value” to existing EU or purely national measures’, p. 27.

⁷⁰ Paula García Andrade, 2015, *op. cit.*, p. 185 ff., underlines that in the lack of an express provision on international treaties in the Protocol No 2, this principle is watched over by the European Parliament. See also Marise Cremona, ‘The External Dimension of the AFSJ’, in Marise Cremona, Jörg Monar, and Sara Poli, *The External Dimension of the European Union's Area of Freedom, Security, and Justice*, Brussels, College of Europe Studies, 2010, pp. 77-118, p. 113, highlighting that the value-added is a ‘version of subsidiarity’.

⁷¹ Paula García Andrade, 2015, *op. cit.*, pp. 188 and 189.

⁷² *Ibidem*, the author does not mention the principle of proportionality, but it may be inferred that this is included in the necessity one according to the analyses made in our previous Chapter.

achieve the Treaty objective of the corresponding internal competence, an objective not to be achieved through the adoption of autonomous rules. This differentiation, which makes it more difficult to exercise concurrent implied external competences than explicit ones, attempts to provide a conciliatory reading of the reinforced necessity criterion established by the Court in *Opinion 1/76* and subsequent case law⁷³.

However, when inferring that the EU external competence is exclusive as soon as the EU finalises an international agreement and that this ‘is necessary to enable the Union to exercise its internal competence’, Article 3(2) TEU is misleading. Prof. García Andrade points out that this norm is actually using the necessity criteria to determine the exclusive nature of the EU external competence, and not its existence, as it should. This provision erroneously incorporates *Opinion 1/76*, as the necessity criteria stemming stands for the ‘indispensability’ of the Union’s intervention to achieve the internal objective. Hence, the author advances the possibility that the norm introduces a new *a priori* form of exclusiveness contrary to the CJEU jurisprudence⁷⁴. Thus, precisely because it is a praetorian doctrine, this rule would allow the CJEU to revisit it and broaden its scope.

In any case, the possibility that the EU’s action can be justified by virtue of the principle of subsidiarity, but not by that of necessity, has crucial consequences on the exercise of such a competence, as the EU is not authorised to solely act externally. In the case of the EU competence on the legal admission of migrants⁷⁵, for instance, Prof. García Andrade comes to the conclusion that the EU could: wait until the upgrading of the level of harmonisation in its internal legislation is complete; conclude a mixed agreement with its Member States, or insert a clause in a wider association agreement by virtue of Article 217 TFEU⁷⁶. In other words, the EU external competence is non-exclusive in the terms analysed below.

1.2.2. External non-exclusive competences

a) Implied external shared competences

Implied external shared competences shall be interpreted *a sensu contrario* from the CJEU’s case-law on the *AETR/ERTA* terms of exclusivity and its developing jurisprudence⁷⁷. In the framework of the doctrine on implied powers, when the EU does not have exclusive

⁷³ Paula García Andrade, 2018, *op. cit.*, p. 174.

⁷⁴ *Ibid.*, p. 182.

⁷⁵ Article 79(1) TFEU.

⁷⁶ Paula García Andrade, 2018, *op. cit.*, p. 176.

⁷⁷ It shall be noted that this rationale is also applicable to express external competence according to the provisions of the founding Treaties, yet for the purposes of this research implied external competence remains our point of reference.

competence to act externally – either because it lacks an *AETR/ERTA* exclusivity, or because its intervention is not necessary by virtue of *Opinion 1/76* – the EU external competence is shared with the one of its Member States. In this sense, the EU action can be deemed to be necessary, though not exclusive, in the following circumstances.

- When the EU has adopted internal rules, the external competence is shared when the envisaged international agreement to be concluded neither affects them, nor alters their scope. This hypothesis includes the primary example of minimum rules or framework dispositions⁷⁸: Minimum rules or framework dispositions are a very peculiar case in which a *de minimis* harmonisation always allows Member States to adopt more stringent rules – i.e., ‘granting more favourable treatment to their beneficiaries’⁷⁹ – than those adopted by the EU, provided that national norms do not prejudice the general objectives pursued by the EU in a specific domain⁸⁰. Thus, Member States are prevented from committing to external relations in cases where the envisaged agreement imposes more stringent rules than the ones internally adopted by the EU, as the Union may decide to raise its minimum standard above the absolute one agreed by the Member States with a third party⁸¹.

⁷⁸ *Opinion 2/91*, para. 18, and also *Opinion 1/03*, paras. 123 and 127. On frame legislations, Robert Schütze, “Classifying EU competences: German Constitutional Lesson?”, in Sacha Garben and Inge Govaere, *The division of competences between the EU and the member States*, Oxford, Hart Publishing, 2017, pp. 33-58, p. 41, points out that these shall accomplish two restrictions: a quantitative and a qualitative one. The former establishes that harmonisation norms shall not be more numerous than those developed to regulate the supplementary action of the state. The latter implies that within a frame legislation exhaustive (or detailed) norm shall respond to the principle of necessity; in his words: ‘[...] Only where detailed provisions were ‘virtually indispensable’ for the operation of the legislative scheme as a whole would the federal legislator be entitled to adopt the act’.

⁷⁹ See Paula García Andrade, 2018, *op. cit.*, p. 172.

⁸⁰ Teresa Fajardo del Castillo, *La política exterior de la Comunidad Europea en materia de medio ambiente*, Ph.D. dissertation, Granada, 2002, p. 290, footnote No. 215, clearly explains that: ‘The reason for this is that Community competence for the environment allows Member States to take more stringent measures at national level in the exercise of their own competences as long as this does not undermine the objectives of general Community policies’ (the translation is ours). According to Adam Tizzano, *op. cit.*, p. 422, in the field of non-exclusive competences, when the founding Treaties expressly limits the EU intervention to the adoption of minimum standards, then, Member States cannot respect such a standard, but they remain free to maintain or introduce more stringent measures than the ones adopted by the EU. In the other cases, the limits imposed to the Member States in the exercise of a shared competence is entirely left to the institutions’ willingness in establishing the range of regulating a specific field.

⁸¹ Paula García Andrade, 2015, *op. cit.*, pp. 158 and 159, and Geert De Baere, 2020, *op. cit.*, p. 106. The latter coincides in that if minimum norms are adopted only by EU secondary law while the international agreement foresee more stringent rules, then, the celebration of bilateral agreements with third countries by the Member States would impede the EU to adopt stricter internal rules than those agreed internationally. Specifically, the possibility that the international agreement foresees only ‘minimum rules’ should be visible thanks to the insertion of clauses allowing the Member States to adopt higher parameters.

- If internal norms have partially harmonised the material domain⁸², or part of the material domain, that is covered by the international agreement by virtue of *Opinion 1/94*⁸³.
- When the internal legislation does not cover the corresponding relevant policy to a large extent, *a sensu contrario* from *Opinion 1/92*⁸⁴.

It is relevant to note that in all the above cases, the EU *acquis* is perceived to be in a *dynamis* status and that as a result, what can be classifiable as shared implied external competence in any particular moment may turn out to be exclusive, unless the underlying legal basis expressly forbids it⁸⁵. This circumstance requires special attention from the Member States due in part to the principle of loyal cooperation of Article 4(3) TEU⁸⁶. Besides, when the EU is entitled to a shared implied external competence with its Member States, it is not prevented from acting alone in compliance with the principle of subsidiarity, though it may decide to exercise it together with its Member States – i.e., in a mixed manner⁸⁷. As the CJEU observed in the case

⁸² *Opinion 2/00*, para. 22 ff. See Paula García Andrade, 2018, *op. cit.*, p. 172 ff., classifying the EU competence on legal migration sets forth under Article 79 TFEU: '[t]his minimal harmonization is clearly detrimental to the EU's external action on migration, since minimal internal rules exclude "affectation" in the sense of ERTA exclusivity provided that potential agreements also contain minimal rules. EU external competences on legal migration are thus concurrent, but the possibility to exercise them is not straightforward'.

⁸³ See also the analysis realised by Paula García Andrade, "The EU Accession to the Geneva Convention Relating to the Status of Refugees: Legal Feasibility and Added Value", *The Spanish Yearbook of International Law*, No. 23, 2019, pp. 193-211, where the author analyses the scope of the Convention relating to the Status of Refugees signed in Geneva on the 28 July 1951, entered into force on 22 April 1954, *U.N.T.S.* No. 2545, Vol. 189, p. 137, to affirm that notwithstanding the level of harmonisation reached by the EU at the internal level, the accession to it will remain a shared competence between the EU and its Member States since the latter retain the competence to examine asylum applications, p. 201.

⁸⁴ C-471/98, *Commission of the European Communities v Kingdom of Belgium*, para. 75 ff.

⁸⁵ Paula García Andrade, 2015, *op. cit.*, p. 184: '[...] this situation is provisional. For if the EU adopts common rules on the matter or if it becomes largely covered by common rules in the sense given by the case law of the CJEU, we will have to carry out again the analysis resulting from the ERTA doctrine with the possibility of affirming the exclusivity of the Union's external competence' (our own translation).

⁸⁶ C-266/03, *Commission of the European Communities v Grand Duchy of Luxemburg*, 2 June 2005, EU:C:2005:341. Prof. García Andrade, 2015, *op. cit.*, p. 202, recalls that: '[...] in areas of shared external competence, compliance with the principle of loyal cooperation requires Member States to consult the Commission when they wish to negotiate an agreement on a subject for which the Commission has received a negotiating mandate from the Council' (the translation is ours). The author comes to the conclusion that in case Member States cannot undertake negotiations on the same fields covered by the Council's mandate, otherwise the EU's influence during the negotiations may be vitiated.

⁸⁷ Mixed agreements are needed when neither the EU nor the Member States participating in the agreement have full competence, including for its implementation, for example, when an international agreement covers several competences of differing natures as the CJEU found in *Opinion 2/15*, 16 May 2017, EU:C:2017:376. However, Member States mixed agreements are also used when the principle of subsidiarity does not allow the EU to solely act externally in case of shared competences, or because the political sensitivity of the area covered by the agreement makes them eventually push to take part in it. On mixed agreement see, for example: Eleftheria Neframi, "Mixed Agreements as a source of European Union Law", in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *op. cit.*, pp. 325-352; Ramses A Wessel, "Cross-pillar Mixity", in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *op. cit.*, pp. 30-54; Marc Maresceau, "A Typology of Mixed Bilateral Agreements", in Christophe Hillion and Panos Koutrakos, *Mixed Agreements Revisited: The EU and its Member States in the World*, Oxford, Hart Publishing, 2010, pp. 11-29; Frank Hoffmeister, "Curse or Blessing? Mixed Agreements in

of the adherence of the EEC to the Fourth African Caribbean and Pacific Countries-European Economic Community Lomé Convention: ‘Since the Community's competence in the field of development aid is not exclusive, the Member States are entitled to enter into commitments themselves vis-à-vis non-member States, either collectively or individually, or even jointly with the Community’⁸⁸.

b) Parallel competences

The concept of “parallel competences” is used to distinguish those cases where the EU and the Member States safeguard their treaty-making power so that an international agreement concluded by one party does not prevent the other from doing the same⁸⁹. This type of external competence stems from several sources, not only the doctrine on implied external competences:

- first, in case of express external competences, parallel competences are generally identified thanks to the expression “without prejudice to” regarding the Member States’ intervention – e.g., development cooperation or humanitarian aid⁹⁰;
- second, parallel competences exist in case the EU intervention is internally limited to supporting, coordinating, and complementing the Member States’ action following the *AETR/ERTA* non affectation logic⁹¹, and
- third, when the harmonisation is expressly excluded by the relevant legal basis notwithstanding its express or implied nature⁹².

2. The European Union’s competence on the protection of personal data and on the free movement of such data: The existence and nature of the European Union’s external action

In Chapter I we learned that before Lisbon, the EU had no express competence on the protection of personal data and on the free movement of such data. This did not prevent the adoption of regulations on the matter: the DPD was adopted under the positive integrationist logic to harmonise Member States’ legislations within the internal market project by virtue of

Recent Practice”, in Christophe Hillion and Panos Koutrakos, *op. cit.*, pp. 249-268, and David O’Keeffe and Henry G. Schermers, *Mixed Agreements*, Deventer, Kluwer, 1983.

⁸⁸ C-316/91, *European Parliament v Council of the European Union*, 2 March 1994, EU:C:1994:76.

⁸⁹ Note that in the English literature is used also the term of ‘concurrent’ which, in our view, is misleading if it is considered that the term ‘concurrente’ among Italian scholars refer to shared competences.

⁹⁰ Articles 208 and 214 TFEU respectively.

⁹¹ Article 2(5) TFEU.

⁹² *Opinion 1/03*, para. 132, where the CJEU did not exclude the existence of an EU external competence *tout court*, yet it was pointing out that such an agreement should have been limited to non-harmonisation clauses so as not to displace Member States’ competences, both internally and externally.

Article 100a of the 1992 TEC⁹³, while the DPF was adopted within the ex-third pillar framework based on Articles 30, 31 and 34(2)(b) of the 1997 TEU that empowered the EU to adopt measures for the ‘collection, storage, processing, analysis and exchange of relevant information, [...] subject to appropriate provisions on the protection of personal data’⁹⁴.

While the intergovernmental framework surrounding the DPF considerably limited the conclusion of international agreements on the EU’s behalf since its international subjectivity was questioned⁹⁵ and, in any case, it could neither act within the *acquis communautaire*⁹⁶, nor respond to the CJEU unless its jurisdiction had been expressly accepted⁹⁷, the (then) European Community could have acquired exclusive competence to act externally on the basis of a “general legal basis” – i.e., Article 100a of the 1997 TEC – only once the internal power had been exercised⁹⁸.

⁹³ See Chapter I.

⁹⁴ Article 30(1)(b) of the 1997 TEU.

⁹⁵ The issue of the EU legal personality was debated on the occasion of the project on a European Constitution (Article I-7 of the Treaty of Rome of 29 October 2004) and has been positively confirmed by the study conducted by Gloria Fernández Arribas, *Las capacidades de la Unión Europea como sujeto de Derecho Internacional*, Granada, Granada Educatori, 2010. In this sense, Marc Maresceau “Bilateral Agreements concluded by the European Community”, *Collected Courses of the Hague Academy of International Law*, Vol. 309, 2004, pp. 125-452, p. 152, explains:

‘It is difficult to imagine that the Council – which concludes such agreements – is only speaking on behalf of the EU Member States, unless the preparatory works of the agreements or the agreements themselves so indicate. If Member States are of the opinion that the EU has nothing to do with a certain issue, they should not “use” the Council; they may conclude agreements with third parties as a group of individuals subjects of international law [...]’.

⁹⁶ Alicia Cebado Romero, “La peculiaridad de la Acción Exterior de la Unión Europea”, in Antonio Remiro Brotons and Irene Blázquez Navarro, *El Futuro de la Acción Exterior de la Unión Europea*, Valencia, Tirant Lo Blanch, 2006, pp. 73-100, p. 80, affirms that: ‘[...] International agreements of the EC differ from those of the EU for the way in which they enter into States’ juridical framework, for the effects they have in these frameworks, as well as the procedure for their celebration’ (our own translation). Article 38 of the 1997 TEU was backed up by Article 24 of the 1997 TEU of the previous Title V on the CFSP. According to this norm:

‘When it is necessary to conclude an agreement with one or more States or international organisations in implementation of this Title, the Council, acting unanimously, may authorise the Presidency, assisted by the Commission as appropriate, to open negotiations to that effect. Such agreements shall be concluded by the Council acting unanimously on a recommendation from the Presidency. No agreement shall be binding on a Member State whose representative in the Council states that it has to comply with the requirements of its own constitutional procedure; the other members of the Council may agree that the agreement shall apply provisionally to them. The provisions of this Article shall also apply to matters falling under Title VI’.

⁹⁷ Article 35 of the 1997 TEU where the European Parliament was excluded from the negotiations. While an agreement based on the ex-first pillar – e.g., Article 95 of the 1997 TEC – would have enabled the European Community to take the lead over the Member States under the Council’s qualified majority approval and the involvement of the European Parliament’s during the negotiations following the implied powers theory, under the ex-third pillar – specifically, Articles 24 and 38 of the 1997 TEU – the unanimity in the Council was required so as to authorise the openness of the negotiations as well as for the conclusion of the agreement, with the sole exception of the agreements concluded for implementing a joint action or a common positions. Hence, the conclusion of any international agreement under the former third pillar was subjected to the domestic constitutional procedure – Article 24 of the 1997 TEU – as Marc Maresceau, 2004, *op. cit.*, pp. 298-304, explains.

⁹⁸ See *Opinion 1/94*, para. 87. Geert De Baere, 2008, *op. cit.*, p. 59, finds that Articles 94, 95 and 308 of the 1997 TEC had been used also to exercise the EU external competence in the absence of an internal legislation – e.g., in environmental law, development cooperation, and economic, financial, and technical cooperation –, yet he

However, the DPD approximated the Member States' national laws while granting them a huge margin of discretion in its implementation and application⁹⁹. In *Lindqvist*¹⁰⁰ Member States asked the CJEU whether they could introduce more stringent national rules to guarantee the greater protection of personal data or with a scope wider than the one set forth by the DPD. The CJEU replied that the DPD generally set forth a complete level of harmonisation to ensure a high level of protection for the processing of personal data, but that Member States kept a certain margin of manoeuvre in some specific areas for which they could maintain or introduce *ad hoc* rules. Similarly, in *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert, Immo 9 SPRL, Grégory Francotte*, the CJEU affirmed that Member States were not obliged to transpose the limitations foreseen on the individuals' rights¹⁰¹ as '[...] the legislator intended to give them the freedom to decide whether, and if so for what purposes, they wish to take legislative measures aimed at limiting, inter alia, the extent of the obligations to inform the data subject'¹⁰². Specifically, in *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*¹⁰³, the CJEU observed that Articles 22 to 24 DPD did not exhaustively regulate existing judicial remedies against the author having committed a breach to the data protection legislation

interprets the CJEU as meaning that in those cases the external action could only be shared. In this regard, we can recall the PNR Agreement with the US, though invalidated by the CJEU, was concluded on the basis of Article 100a of the 1997 TEC.

⁹⁸ Marc Maresceau 2004, *op. cit.*, p. 198.

⁹⁹ Alison White, "Control of Transborder Data Flow: Reactions to the European Data Protection Directive", *International Journal of Law and Information Technology*, Vol. 5, No. 2, pp. 230-248, 1997, p. 239, noted that: 'To the extent that the Directive permits derogations it cannot be said to be a true harmonisation measure yet its aim is to provide an equivalent level of protection throughout the Union'. Paul M. Schwartz, *loc cit.*, instead, observed that:

'[...] most European nations require "equivalency" in foreign lands before permitting international data transfers. The Directive defines a standard of "adequacy," which sets out a more lenient requirement. If the Directive sets out only minimum standards, it will permit Member States to enforce their higher standards for international data transmission. The Council of Europe's Convention takes this approach; it sets only minimum standards'

On the same wave lie Graham Pearce and Nicholas Platten, *op. cit.*, p. 544:

'Progress has indeed been remarkable, but doubts remain about the practicalities of harmonizing and applying data protection laws. Establishing an agreement in the form of a directive marks only the first stage and within the EU there remain concerns about the way it may be transposed into national laws and applied in each Member State. Much of the vocabulary of the directive is abstract and it may take many years for a body of interpretative CJEU law to develop. In the meantime, this places particular responsibility on the Article 29 working group of Member State Data Protection Commissioners, which will be responsible for policing and advising on implementation procedures. In addition, the European Commission will play a key part in implementation, through the 'Article 31' comitology group, which authorizes it to make decisions on data transfers to third countries'. Thus far, however, no definitive answer can be given as to whether the Directive takes this approach'.

¹⁰⁰ C-101/01, *Bodil Lindqvist v Åklagarkammaren i Jönköping*, para. 82.

¹⁰¹ Namely Article 13 DPD, now Article 23 GDPR.

¹⁰² C-473/12, *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert, Immo 9 SPRL, Grégory Francotte*, para. 32.

¹⁰³ C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*.

and validated the German Law allowing customer associations to bring judicial challenges in the interest of the data subject, although this was not expressly provided in the EU legislation¹⁰⁴. Conversely, in *Mehrdad Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEDM) v Administración del Estado*¹⁰⁵, the CJEU was called upon to interpret the principle of lawfulness enshrined in Article 7(f) DPD¹⁰⁶ and it emphasised that the catalogue of cases listed therein should have been considered as exhaustive, and Member States should not have added new principles relating to the lawfulness of the processing of personal data nor added further requirements to those foreseen by EU law. The CJEU added that this provision was sufficiently precise and unconditional to deploy direct effect in the Member States' legal orders¹⁰⁷.

According to the Article 29 DPWP¹⁰⁸ and the EDPS¹⁰⁹, the level of approximation achieved by the DPD was as minimum as possible which resulted in serious distortive effects because of its divergent transposition in Member States' law. Recital (9) DPD is significant in this regard as it contemplated the fact that '[...] within the limits of this margin for manoeuvre and in

¹⁰⁴ The CJEU observed that currently the GDPR expressly provides for it in its Article 80(2) GDPR.

¹⁰⁵ C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEDM) v Administración del Estado*, 24 November 2011, EU:C:2011:777.

¹⁰⁶ Current Article 6(1)(f) GDPR.

¹⁰⁷ C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEDM) v Administración del Estado*, paras. 50-55. Similarly, in C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, 19 October 2016, EU:C:2016:779, the CJEU considered that the German Law unlawfully restricts Article 7(f) DPD as far as the process of International Protocol addresses was concerned. According to this law, an online media services provider might collect, use, and charge for, a user's personal data without his consent only to the extent necessary in order to facilitate the specific use of those services by the user concerned, and under which the purpose of ensuring the general operability of those services cannot justify use of the data beyond the end of the particular use of them. The CJEU ruled that the General Federal Institutions might have had a legitimate interest in guaranteeing the continued functioning of those websites so that the national legislation was truly not clarifying what "general interest" consisted in, but it was *a priori* preventing the balancing between the legitimate interest pursuit and the fundamental rights at stake. All in all, such legislation was reducing the scope of application of Article 7(f) DPD by intruding further limitations to one of the principles derogating from the necessity of the consent of the data subject to lawfully process personal data.

¹⁰⁸ See, for example, the Opinion of the Article 29 DPWP No. 10/2004 on *More Harmonised Information Provisions*, Brussels, 25.11.2004, that complained about the different transpositions of DPD as far as the right to information of the data subject is concerned, and the Report of the Article 29 DPWP on *the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union*, Brussels, 18.01.2005. Also, the *Strategy Document*, Brussels, 29.09.2004, that sets within its priorities the harmonised compliance with DPD standards.

¹⁰⁹ See the Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, OJ C 255, 27.10.2007, pp. 1-12, that urged the European Commission to undertake infraction procedures where necessary, and the Opinion of the EDPS on *the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"*, Brussels, 14.01.2011, p. 12 ff., where it suggested to: reduce Member States' margin of manoeuvre in implementing DPD; prevent incorrect implementation, and ensure more consistent and coordinated enforcement.

accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community'. Therefore, affirming the applicability of the *AETR/ERTA* effect would be quite daring on our part. The internal legislation was minimally and partially harmonising¹¹⁰ the field at issue and, in the external layer, Member States remained free to conclude international agreements without undermining the European Community's rules, or altering their scope¹¹¹. In the specific case of the international data transfer regime, the analysis is even easier, as Article 25 DPD acknowledged to both the European Commission and its Member States¹¹² – specifically, data protection authorities and data controllers – could conduct an “adequate evaluation”¹¹³, but they were called to cooperate anyway¹¹⁴. The DPD foresaw the possibility to derogate from the adequacy parameter for the specific reasons set forth therein¹¹⁵

¹¹⁰ Marcus Klamert, “What We Talk About When We Talk About Harmonisation”, *Cambridge Yearbook of European Legal Studies*, No. 17, 2015, pp. 360-379, distinguishes between full and partial harmonisation, on the one hand, and maximum and minimum harmonisation on the other one. According to the author:

‘Harmonisation is ‘full’ in scope when there is comprehensive or exhaustive legislative harmonisation in a specific area; harmonisation will otherwise be said to be ‘partial’ in scope. But, distinct from the scope of harmonisation, the standard(s) set by European legislation may also vary in their intensity. They may provide for ‘full (or ‘maximum’, or ‘total’)' harmonisation, in the sense of setting standards which Member States cannot derogate from, or they may provide for ‘minimum’ harmonisation only, leaving some discretion to Member States in, for example, setting a higher standard than the minimum standard(s) adopted under European law’.

¹¹¹ For this reason, the Article 29 DPWP guided an Enforcement Task Force since 2004 in order to understand the level of implementation of the DPD in the Member States and improving its compliance – see the Report of the Article 29 DPWP No. 1/2007 on *the first joint enforcement action: evaluation and future steps*, Brussels, 20.06.2007, and Id., *Mandate to the Enforcement Subgroup to proceed to the 2nd joint investigation action*, Brussels, 17.07.2008. In 2009, the Article 29 DPWP, *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, Brussels, 1.12.2009, highlighted how Member States still differently implemented DPD, for example, in the fields of the responsibility of data controllers and the empowerment of national supervisory authorities, though it suggested that uniform application of DPD may have been achieved by the own body while publishing stringent guidelines. Also, the principle of purpose limitation had been divergently interpreted by the Member States as it is analysed in the Opinion of the Article 29 DPWP No. 03/2013 on *purpose limitation*, Brussels, 2.04.2013, p. 10.

¹¹² Member States could have established *ex ante* checks burdening upon data controllers or *ex post* controls to be conducted by the supervisory authority according to the Working Document of the Article 29 DPWP, *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, Brussels, 07.1998, p. 27.

¹¹³ Member States had the choice on how to conduct an adequacy assessment under Article 25 DPD – see the Working Document of the Article 29 DPWP on *a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, Brussels, 25.11.2005, where it was urged that derogation clauses should have been chosen always as a last option contrary to what controllers were doing in practice, p. 7. Article 25 DPD required Member States to communicate the European Commission cases in which a third country was estimated to not accomplish with adequate standards and the European Commission, for its part, should have widespread to the whole Member States the news that a third country was found to be not conform with adequate standard.

¹¹⁴ Article 25(3) DPD.

¹¹⁵ Article 26 DPD, see also the analysis of the Working Document of the Article 29 DPWP, *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, Brussels, 07.1998, pp. 24-25.

or by means of contractual clauses¹¹⁶. Only in the latter case were Member States obliged to notify the European Commission in order to gain its approval¹¹⁷. Consequently, the European Commission had no monopoly over the determination of the adequacy of data protection standards, which has important consequences on the binding nature of the European Commission's decision *vis-à-vis* data protection authorities¹¹⁸.

After the Lisbon Treaty entered into force, there is no doubt that the EU is conferred an express shared competence on the protection of personal data and on the free movement of such data. Article 16(2) TFEU has an internal introspection directed at the regulation of the processing activities of Member States and EU institutions, bodies, offices, and agencies '[...]' when carrying out activities that fall within the scope of Union law'. On this legal basis, from 2016 onwards, the EU has developed its own data protection *acquis*¹¹⁹. As Prof. Wyatt and Prof. Dashwood highlight, "internal provisions" acquire an external projection in application of the *AETR/ERTA* doctrine by its exercise or, alternatively, according to the strict necessity requisite enshrined in *Opinion 1/76*¹²⁰. The following paragraphs analyse the existence and nature of an EU competence on the protection of personal data and on the free movement of such data based on Article 16(2) TFEU. First of all, we will assess the existence of the EU external competence in the field of personal data protection and free movement¹²¹ for which purpose we must identify the main objective/s pursued internally on the basis of Article 16(2) TFEU, as well as the necessity of EU external intervention to achieve such a goal. Following

¹¹⁶ Article 26(2) DPD, see also the comments of the Working Document of the Article 29 DPWP, *Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries*, Brussels, 22.04.1998, and the Opinion of the Article 20 DPWP No. 1/2001 on the *Draft Commission Decision on Standard Contractual Clauses for the transfer of Personal Data to third countries under Article 26(4) of Directive 95/46*, Brussels, 26.01.2001.

¹¹⁷ Article 26(3) and (4) DPD. On the adequacy decision under the DPD see Francis Aldhouse, "The Transfer of Personal Data to Third Countries Under EU Directive 95/46/EC", *International Review of Law Computers & Technology*, No. 1, Vol. 13, 1999, pp. 75-79.

¹¹⁸ For example, in the case of the Safe Harbour Agreement see Rolf H. Weber, *op. cit.*, p. 127, and *infra*.

¹¹⁹ See Chapter I.

¹²⁰ Alan Dashwood, Michael Dougan, Barry Rodger, Eleanor Spaventa, and Derrick Wyatt, *op. cit.*, p. 913 ff., the latter case is labelled as 'complementary principle' since: '[...] implied competence to enter into international commitments is explained as a necessary complement of the internal competence flowing from the relevant legal basis'. Prof. Matera notes that in the AFSJ the EU competences in the freedom section are 'open provisions' according to Dashwood's systematisation so that even though they have an intrinsically external projection, they do not confer to the EU an express empowerment to celebrate international agreement – Claudio Matera, *The External Dimensions of the EU Area of Freedom, Security and Justice: A Constitutional Perspective*, Ph.D. dissertation, University of Twente, 2016, p. 132 ff. The sole exception is Article 79(2) TFEU that expressly confer the EU the competence to conclude readmission agreements. On the contrary, the EU competences on judicial cooperation in civil matters are 'internal provisions' which – as *Opinion 2/00*, 6 December 2001, EU:C:2001:664, testifies – does not prevent the EU from acting externally according to the doctrine on implied powers. Similarly, internal provisions characterise the criminal areas, apart from the fact that some of the freedom, security and justice agencies were expressly allowed to conclude binding agreements with third countries as we analyse in due course.

¹²¹ Paula García Andrade, 2015, *loc. cit.*

this, we will assess the nature of the EU external competence by applying the doctrine of implied powers in the terms developed by the CJEU jurisprudence.

We will take into account the degree of harmonisation achieved by the EU instruments after the Lisbon Treaty to see whether the internal shared competence based on Article 16(2) TFEU has become an *AETR/ERTA* exclusivity, which would prevent the Member State from acting externally – as has been already advanced by other experts¹²² – or not. The possibility that Member States introduce national standards, including more stringent measures, than those established by the EU in the GDPR and the LED respectively, shall be analysed in the light of the CJEU jurisprudence, according to which Member States must not undermine the primacy, unity, and effectiveness of EU law¹²³.

2.1. The necessity of European Union's intervention to attain the objectives pursued by Article 16 of the Treaty on the Functioning of the European Union

If it is assumed that the competence of the Union sealed under Article 16(2) TFEU not only aims to guarantee the protection to individuals' personal data, but also of ensuring its free movement, then, both components must integrate the EU external action and, specifically, the regime set forth to transfer personal data internationally. It may be understood, as was explained in the previous Chapter, that the Lisbon Treaty gives more weight to the respect of individuals' fundamental rights than before, as the link between Article 16(1) TFEU and Article 8 of the CFREU has been strengthened since the 2007's reforms. Yet, this does not change the fact that the EU competence on personal data sealed under Article 16(2) TFEU carries a twofold purpose, that is, the protection of personal data and the free movement of such data. Both the GDPR and the LED expressly include within their objectives the protection of natural persons with regard to the processing of personal data in the light of Article 8 of the CFREU, as well as the 'free movement of such data' or the 'exchange of personal data' respectively¹²⁴.

Notably, Chapter V of the GDPR and Chapter V of the LED attribute to the EU's external action a specific objective for which the level of protection granted by the EU data protection

¹²² Hielke Hijmans, 2016, *loc. cit.*

¹²³ C-617/10, *Åklagaren v Hans Åkerberg Fransson*, para. 19, and *Opinion 2/13*, para. 189, the latter affirming the draft agreement on the accession of the EU to the ECHR was not compatible with Article 6(2) TEU.

¹²⁴ Articles 1 GDPR and 1 LED respectively.

legislation shall not be undermined through the disclosure of personal data to third countries and international organisations¹²⁵. According to Article 44 GDPR:

‘Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined’.

This clarity is due to the fact that, unlike the DPD, the GDPR openly addresses personal data as a fundamental right domain, releasing it from the achievement of internal market objectives¹²⁶. As it was analysed in the former Chapter, this change is supported by both an express data protection competence conferred to the EU under Article 16(2) TFEU, as well as the provision of the fundamental right to the protection of personal data under Article 8 of the CFREU recalled in Article 16(1) TFEU. Under the aegis of the universal recognition of the fundamental right to the protection of personal data, the GDPR has an ambitious scope that overrides the internal market, this includes:

- the AFSJ and an economic union;
- the economic and social progress;
- the strengthening and the convergence of the economies within the internal market, and
- the well-being of natural persons¹²⁷.

Therefore, although recognising the need to exchange data with third countries and international organisations¹²⁸ for the expansion of international trade as well as – which is new – to support general international cooperation¹²⁹, the GDPR sets forth a non-exhaustive list of tools legitimising the international transfer of personal data, that covers the private and public sectors¹³⁰.

¹²⁵ Articles 44 to 50 GDPR. International data transfer shall be distinguished from the so-called ‘cross-border processing’ that according to Article 4(23) GDPR concerns the processing of personal data that has an impact on two or more Member States because of the controllers or processors activities, or the data subjects affected by it.

¹²⁶ Article 1 GDPR.

¹²⁷ Recital (2) GDPR.

¹²⁸ The transfer of personal data to international organisations was not foreseen in the DPD. Articles 4(26) GDPR and 3(16) LED expressly provide an own definition of international organisation for which: ‘[...] an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries’.

¹²⁹ Recital (101) GDPR.

¹³⁰ Chapter V GDPR.

Despite Member States' concerns¹³¹, the EU legislation does not clarify whether the expression "transfer" includes also other forms of cooperation activities that can make data available to other parties – e.g., the 'exchange of personal data' or the 'disclosure of personal data'¹³². Recital (101) of the GDPR recognises the double track of data, that both goes to and comes from countries outside the Union and international organisations, as a necessary feature for the expansion of international trade and cooperation, but the attention of the co-legislator under Chapters V of the GDPR and that of the LED focuses on the unilateral flow of data – i.e., from the EU to third parties only. As the EDPS underlined, clarifying the concept of "data transfer" is most urgent in the face of the increasing use of new forms of data sharing – e.g., cloud services – for which personal data is not actively transferred, but made available to other recipients worldwide¹³³ and it suggested, for example, to rely on criteria such as the communication or open availability of data, whether the data has been made freely available with the aim of giving access to it, and whether the transfer is likely to reach one or more recipients abroad¹³⁴. In its view, to avoid any circumvention of the internal regime, the concept of international data transfer shall be broadly interpreted so as to include a variety of operations that imply the movement of data between different users, such as '[...] communication, disclosure or otherwise making available of personal data, conducted with the knowledge or intention of a sender subject to the Regulation that the recipient/s will have access to it. The term would therefore cover both "deliberate transfers" and "permitted access" to data by recipient/s'¹³⁵. The EDPB embraced this position and specified that the three following cumulative conditions must be met in order to qualify an act of processing as a "transfer": first, the controller or processor exporting the personal data has to be subject to the GDPR; second, the exporter of personal data must transmit it or 'otherwise makes [it] available' to another

¹³¹ See, for example, the Romanian comment that suggested a definition of "transfer" in Council of the EU, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Comments on Chapter V*, 6723/5/13 REV5, Brussels, 12 December 2013, p. 107.

¹³² See Christopher Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford, Oxford University Press, 2013, pp. 11-14, who relies on the terms "transborder data flows" according to the OECD Privacy Guidelines and the Convention 108 to exclude the mere "transit" of data in and out the by virtue of Article 4(1)(C) DPD, yet this disposition was not inserted in the new GDPR.

¹³³ See the Opinion of the EDPS on *the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"*, Brussels, 16.11.2012, p. 17. Querying the establishment of the competent jurisdiction as well as the law applicable to contractual relationship involving transborder clouds is Gianpaolo Maria Ruotolo, "Hey! You! Get OV My Cloud! Accesso autoritativo alle nuvole informatiche e diritto internazionale", *Archivio Penale*, No. 3, 2013, pp. 853-864.

¹³⁴ See the Opinion of the EDPS on *the data protection reform package*, Brussels, 7.03.2012, p. 19.

¹³⁵ See the Position Paper of the EDPS, *The transfer of personal data to third countries and international organisations by EU institutions and bodies*, Brussels, 14.07.2014, p. 7.

controller or processor and, third, the importer of the personal data shall lie in a third country, or shall be an international organisation ‘[...] irrespective of whether or not this importer is subject to the GDPR in respect of the given processing in accordance with Article 3’¹³⁶. On closer inspection, a broad interpretation of the concept of “transfer” is the only one that ensures that the international flow of personal data runs safely among different actors that share global data protection standards. The EDPB excluded from the definition of “transfer” cases where the data subject discloses his/her personal data to the recipient directly, which is in line with the (controversial) CJEU’s finding in *Lindqvist*. According to the latter, the publication of personal data on the Internet could have not been interpreted as falling into the data transfer regime foreseen in Chapter II of the DPD¹³⁷: the CJEU noted that the information should be considered to have been sent by the computer infrastructure of the hosting provider where the page was stored and did not represent a person-to-person transfer of personal data – i.e., from Ms. Lindqvist to each webpage client. The CJEU highlighted that by considering the publication of information on the Internet as a transfer of personal data to third countries, it should not have not been uploaded on to the web in case a single country was found to have inadequate protections in place. However, this judgment might be interpreted as excluding from the EU regime on the transfer of personal data any disclosure performed by an IT system which risks leaving a huge regulatory gap in our view.

Derogations to the international transfer regime set forth by the GDPR concerns the processing activities conducted in the frame of PJCCM by virtue of Declaration No 21, that is, the LED¹³⁸. Although acknowledging that the protection of personal data lies at the core of the LED, the co-legislators point out that Member States are the only ones in charge of safeguarding the individuals’ fundamental right to the protection of personal data, as well as its exchange, by virtue of the Member States’ domestic laws¹³⁹. While transposing the LED, Member States shall specify that the transfer of personal data to third countries and international organisations is directed to the purposes of prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the safeguard against and the prevention of threats to public security, which also delimits the data protection controller

¹³⁶ See the Guidelines of the EDPB No. 05/2021 on *the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, Brussels, 18.11.2021, p. 4 ff. The EDPB warns that the EU regime on the transfer of personal data applies also in case the data controller or processor is established outside the EU, but this is subject to the GDPR by virtue of its Article 3.

¹³⁷ C-101/01, *Bodil Lindqvist v Åklagarkammaren i Jönköping*, para 63.

¹³⁸ Articles 35 to 40 GDPR.

¹³⁹ Article 1(2) GDPR.

legitimised to receive the data¹⁴⁰. The LED undertakes the DPFDR rationale in case the personal data to be transferred has been obtained from another Member State¹⁴¹, accordingly, the authorisation of the latter is necessary, except for cases of ‘immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member States’¹⁴². Nevertheless, Article 35(3) LED recalls that all provisions set down in Chapter V ‘[...] shall be applied in order to ensure that the level of protection of natural persons ensured by this Directive is not undermined’. In other words, the LED follows the GDPR’s lead while confirming that the regime on the transfer of personal data pursues a specific objective consisting of the prevention of any activity or legislation that circumvents internally established data protection standards – or *fraude à la loi*¹⁴³.

Taken as such, it may be argued that the concept of non-circumvention only refers to the protective elements of the EU competence of Article 16(2) TFEU, while setting aside the need of free movement of personal data. Regarding the vagueness of the concept of “circumvention”, Prof. Kuner points out that this requisite cannot constitute the sole objective justifying the transborder flow of data¹⁴⁴. Specifically, he suggests keeping such a concept as an aggravating factor, for example, when the data transfer demonstrates bad faith or violates a strong public policy. The author advances three main reasons that may potentially spur the adoption of transborder data flow regulation on the part of the EU.

First, the author assumes that regulating the transfer of personal data lowers the risks presented by data processing activities conducted abroad. The outsourcing of data processing activities to third countries with unstable democratic systems harshens the flow of data when it is discovered, for example, that law enforcement authorities have disproportionate access to the data. Such a point is usually made by those states whose practices are most questionable *vis-à-vis* their national data protection legislation – namely, the United Kingdom and Germany¹⁴⁵. These two states seem to instrumentalise the data protection discourse to hinder the spreading of information, which gives rise to inequality if states that do not possess strong intelligence services do not have access to the information possessed by those who do. The regulation of

¹⁴⁰ Article 35(1)(a) and (b) LED.

¹⁴¹ Article 13(1) DPFDR.

¹⁴² Article 35(1)(c) and (2) LED.

¹⁴³ Dan Svantesson, “Enforcing Privacy Across Different Jurisdictions”, in David Wright and Paul De Hert, *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, Cham, Springer, 2016, pp. 195-222, p. 105.

¹⁴⁴ Christopher Kuner, 2013, *op. cit.*, p. 107 ff.

¹⁴⁵ See the jurisprudence of the ECtHR analysed in Chapter I.

the transfer of personal data, then, should counter their hostility in cooperating with third parties more than protecting individuals.

Second, Prof. Kuner believes that data transfer regulations counteract the difficulty in asserting rights abroad. This issue has been challenged through a variety of recommendations in international fora – e.g., the Global Privacy and enforcement Network and the Asia-Pacific Economic Cooperation Cross-Border Privacy Enforcement Arrangements –, bilateral agreements, as well as private initiatives¹⁴⁶ and – just as first point – it is usually buffered by extraterritorial provisions. By virtue of Article 3(2) GDPR, data processing activities conducted by a controller or processor, in the context of an establishment settled in a third country fall within the scope of EU law when the processing is moved for economic reasons, or when it is used to monitor the activity of the individuals present within the EU territory¹⁴⁷. In its historical sentence in *Google Spain*, the CJEU found that, despite the fact that Google Spain’s parent company was settled in the US, the company was directing its promotion and sale of advertisement spaces in a Member State and, as a consequence, was subject to the GDPR dispositions¹⁴⁸. However, we should highlight the fact that extraterritoriality is looked at with suspicion by the majority of scholars¹⁴⁹, who are worried about such an overreaching regulation

¹⁴⁶ Hielke Hijmans, 2016, *op. cit.*, p. 116: ‘Conflicts of jurisdiction are an inherent phenomenon on the internet and should be addressed, in relation to third countries that do not share the same democratic values, but also with countries that share many of the values that deserve protection’.

¹⁴⁷ In this case, the data controller or processor shall designate a representative within the EU according to Article 27(1) GDPR except when the processing is occasional, or it is carried out by a public authority or body. See Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson, “The extraterritoriality of data privacy laws—an explosive issue yet to detonate”, *International Data Privacy Law*, No. 3, Vol. 3, 2013, pp. 147-148, and Benjamin Greze, “The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives”, *International Data Privacy Law*, No. 2, Vol. 9, 2019, pp. 109-128. The latter questions the effective enforceability of the EU data protection law to controllers and processors established beyond its borders.

¹⁴⁸ C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González*, para. 51. The CJEU underlined that the DPD did not require the processing to be carried out by the establishment itself but in the context of its activities.

¹⁴⁹ Bernhard Maier, “How Has the Law Attempted to Tackle the Borderless Nature of the Internet?”, *International Journal of Law and Information Technology*, No. 2, Vol. 18, 2010, pp. 142-175, p. 161; Christopher Kuner, “Data Protection Law and International Jurisdiction on the Internet (Part 2)”, *International Journal of Law and Information Technology*, No. 3, Vol. 18, 2010, pp. 227-247, p. 235; Chris Reed, *Making Laws for Cyberspace*, Oxford, Oxford University Press, 2012, pp. 189-204, p. 49, and Lokke Moerel, “The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?”, *International Data Privacy Law*, No. 46, Vol. 1, 2011, pp. 28-46. Only Dan Jerker B Svantesson, “Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation”, *International Data Privacy Law*, No. 4, Vol. 5, November 2015, pp. 226-234, p. 233, supports it while affirming that:

‘[...] extraterritorial jurisdiction claims are reasonable because if states do not extend their data protection to the conduct of foreign parties, they are not providing effective protection for citizens. At the same time, wide extraterritorial jurisdictional claims are arguably unreasonable because it is not possible for those active on the Internet to adjust their conduct to all the laws of all the countries in the world with which they come into contacts’.

that may not be accompanied by appropriate guarantees to ensure the enforceability of data protection safeguards. In these terms, extraterritoriality over cooperation is not the best option, as it does not ensure the protection of personal data of individuals' falling within the EU jurisdiction. For example, the LED does not provide for any disposition on extraterritoriality applicable to third countries' authorities if their activity impacts data subjects settled within the EU, which we find reasonable, as foreign public authorities cannot be unilaterally subjected to EU law.

Third, Prof. Kuner maintains that the EU norms on the transfer of personal data are vital to the enhancement of individuals' trust in the organisation. Although the author finds himself sceptical about this possibility, we believe that this is a crucial factor to take into account in the digital age and, specifically, regarding the internal free movement and external transfer of personal data. Strong regulations that ensure the transborder protection of data rights enable the release of individuals' personal data, which ensures their free (transborder) movement. In other words, we assume that an effective regime on the transfer of personal data is needed in order to boost an internal market where information concerning individuals circulates freely. In these terms, Prof. Kuner succeeds in widening the non-circumvention objective that incorporates the protective and free movement elements of Article 16 TFEU.

Given the above considerations, we assume that cooperation with third countries and international organisations in the field of personal data is indispensable for two reasons. First, the EU must ensure a high level of protection for its citizens' fundamental rights¹⁵⁰, and should provide citizens with effective mechanisms to enforce their data subject rights *vis-à-vis* third parties, both within and beyond its borders¹⁵¹, when its institutions, bodies, offices and agencies as well as its Member States are implementing Union law¹⁵². Therefore, to guarantee compliance with EU law by third parties – and if their activity is directed towards the Union – the EU needs to count on the foreign party's cooperation¹⁵³. Second, the existence of different degrees of protection between Member States – including the European Economic Area (EEA) states¹⁵⁴ – and third countries or international organisations hampers the flow of data – as was

¹⁵⁰ Mistale Taylor, "The EU's human rights obligations in relation to its data protection laws with extraterritorial effect", *International Data Privacy Law*, Vol. 5, No. 4, 2015, pp. 246-256.

¹⁵¹ Federico Fabbrini, Edoardo Celeste, and John Quinn, *Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Oxford, Hart Publishing, 2021, p. 2.

¹⁵² Article 51(1) CFREU.

¹⁵³ See Lingjie Kong, "Data Protection and Transborder Data Flow in the European and Global Context", *European Journal of International Law*, Vol. 21, No. 2, 2010, pp. 441-456.

¹⁵⁴ See the EEA joint committee, *Decision amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol No. 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022]*, No. 154/2018, 6 July 2018. For this purpose, the reference to Member State is intended

the case within the EU before the Member States' domestic legislation was harmonised – means that the EU is called on to cooperate with third parties in order to make foreign legal orders compatible with its own¹⁵⁵. In the absence of universal harmonised data protection standards, approximation with EU standards is necessary so as not to hinder the internal exchange of personal data. Indeed, if standards differ, Member States might decide not to exchange personal data with one another, acknowledging that the shared information could be transferred to third parties that do not provide appropriate safeguards. In addition, if an authority in one Member State does not receive the data requested from another Member State because, for example, there is not a fully harmonised level of protection within the EU, then the former could be tempted to seek the assistance of a foreign country with weaker guarantees – a so-called “data paradise”. A fragmented situation would facilitate “data shopping” under which foreign authorities direct their requests to the most flexible Member State and vice versa¹⁵⁶.

Although recognising the need to exchange information with third countries and international organisations¹⁵⁷ – not only for the expansion of international trade, as the DPD envisaged, but also in order to facilitate international cooperation in line with the GDPR¹⁵⁸ – the GDPR and the LED each set out a non-exhaustive list of tools legitimising the international transfer of personal data, covering the private and public sectors¹⁵⁹. Studying these tools, it is understood that the EU ambition to protect privacy universally is firstly embedded in the so-called “adequacy” or “geographically-based”¹⁶⁰ model that requires Member States not to hamper the flow of information toward third parties offering an adequate level of protection to EU data, and which is backed up by a European Commission's implementing decision. The

as including EEA states since these are not considered as third countries under the regime on the international transfer of personal data.

¹⁵⁵ See the Article 29 DPWP, *First Annual Report*, Brussels, 25.01.1997, p. 17, on the dialogue with third countries on data protection matters. The Article 29 DPWP points out that the improvement of third countries' level of protection should have been a common priority in order to avoid disruptive effects on the worldwide flows of personal data. For its part, Paul De Hert, 2021, *op. cit.*, p. 299, notes that independent supervisory authorities are a continental invention not shared by numerous third countries, above all the US: '[...] in a connected world with international transfers, the EU is using its basic documents to defend its vision on effective enforcement of privacy and data protection, with independent agencies as a major building block'.

¹⁵⁶ Second Opinion of the EDPS on the *Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters*, Brussels, 26.04.2007, para. 22. Kuner, 2013, *op. cit.*, p. 104, well explains that the existence of different regulations worldwide may trigger a ‘race to the bottom’ or a ‘race to the top’ when data are transferred toward a state with a less or a more permissive data protection regime, respectively.

¹⁵⁷ The transfer of personal data to international organisations was not envisaged in the DPD. Article 4(26) GDPR and Article 3(16) LED expressly provide an own definition of international organisation for which: ‘[...] an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries’. We will return to this point in Chapter VI.

¹⁵⁸ Recital (101) GDPR.

¹⁵⁹ Chapter V GDPR.

¹⁶⁰ Christopher Kuner, 2013, *op. cit.*, p. 64 ff.

ability of the EU to intervene unilaterally by making use of the European Commission's implementing powers effects and becomes complicated by the ability of the EU to exercise its treaty-making powers. Specifically, the unusual instrument known as the "adequacy decision" relegates the conclusion of international treaties to an inferior layer, as further analysed below.

2.1.1. Adequacy decisions in the field of the protection of personal data and on the free movement of such data

The double-headed nature of the EU competence on personal data implies that both the protection and the free flow of data follow the so-called adequate level of protection parameter¹⁶¹. This standard was first advanced under the DPD and strictly required Member States to outsource data '[...] only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection'¹⁶². Derogations were allowed for specific reasons set out under Article 26(1) DPD¹⁶³ or by means of contractual clauses¹⁶⁴. The DPDF, for its part, stuck to the First Additional Protocol of 2001 to Convention 108¹⁶⁵ that enabled the Council of Europe's Member States to exchange personal data with third parties in the 'legitimate specific interest of the data subject' or for 'legitimate prevailing interests, especially

¹⁶¹ Article 45 GDPR and 36 LED.

¹⁶² Article 25(1) DPD. On the adequacy decision under the DPD, see Alexander Zinser, "International Data Transfer out of the European Union: The Adequate Level of Data Protection According to Article 25 of the European Data Protection Directive", *John Marshall Journal of Computer and Information Law*, Vol. 21, No. 4, 2003, pp. 547-566, and Francis Aldhouse, *loc. cit.*

¹⁶³ That is, when: the data subject has given his consent unambiguously to the proposed transfer; or the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or the transfer is necessary in order to protect the vital interests of the data subject; or the transfer is made from a register, which, according to laws or regulations, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case. See the Working Document of the Article 29 DPWP, *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, Brussels, 07.1998, pp. 24-25.

¹⁶⁴ Article 26(2) DPD. Yet, in this case, Member States were obliged to notify to the European Commission any transfer activity in order to obtain or not its approval on the contractual clauses adopted, and Member States had to conform to its decision anyway. See the comments in the Working Document of the Article 29 DPWP, *Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries*, Brussels, 22.04.1998, and the Opinion of the Article 20 DPWP No. 1/2001 on the *Draft Commission Decision on Standard Contractual Clauses for the transfer of Personal Data to third countries under Article 26(4) of Directive 95/46*, Brussels, 26.01.2001.

¹⁶⁵ The First Additional Protocol to Convention 108 establishes minimum guarantees on supervisory authorities and transborder exchange of data, but it allowed for broad derogations to the adequacy requirements – confront Article 12.

important public interests’¹⁶⁶. Hence, Member States had to ascertain whether a third country complied with an adequate level of protection on their own¹⁶⁷ and, in any case, the DPF¹⁶⁸ only applied to the processing of personal data previously exchanged or made available among the Member States¹⁶⁸. The existence of a decentralised assessment system on adequacy hampered the uniform application of the EU *acquis* on personal data and, consequently, impeded a consistent EU external action.

Today, provided that adequacy decisions are adopted in conformity with the European Commission’s implementing powers¹⁶⁹, which bind all Member States¹⁷⁰, it is the EU intervention alone that ascertains the lawfulness of transborder transfers of personal data under the GDPR and the LED¹⁷¹. In a nutshell, adequacy decisions require that the law in force in a third country or organisation is “essentially equivalent” to that of the EU so that it can guarantee enforceable rights to EU citizens and residents¹⁷². In case of adoption, adequacy decisions ensure that personal data can be transferred without the need for a previous authorisation, with the sole exception set forth under the LED in case the data to be transferred “belongs” to another Member State¹⁷³.

The concept of “essentially equivalent” has been tailored by the CJEU jurisprudence scrutinising the US level of protection¹⁷⁴ in what is known as the *Schrems* saga. In *Maximilian*

¹⁶⁶ Article 13(2)(a) DPF¹⁶⁸.

¹⁶⁷ Article 13(3)(b) DPF¹⁶⁸. Specifically, it derogates from Article 13(1)(d) DPF¹⁶⁸ for which data transfer was lawful if ‘the third State or international body concerned ensures an adequate level of protection for the intended data processing’. It is difficult however to maintain that the European Commission could have adopted an adequacy decision under the DPF¹⁶⁸ since the latter did not provide any specific provision. A critical view on the DPD regime compared with that of the United Kingdom has been made by Francis Aldhouse, *loc cit*.

¹⁶⁸ Article 13(2) DPF¹⁶⁸. DPF¹⁶⁸ had many other shortcomings carrying the burden of the former third pillar, as we analysed in Chapter I. Among others, we should recall its scope of application, the lack of direct application, the limited powers of the European Commission as well as the CJEU, and the presence of open clauses that prevented the harmonisation of Member States’ internal legislations.

¹⁶⁹ Articles 45 GDPR and 36 LED.

¹⁷⁰ Article 45(3) to (9) GDPR. See, for example, Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen Borgesius, “The European Union general data protection regulation: what it is and what it means”, *Information & Communications Technology Law*, Vol. 28, No. 1, 2019, pp. 65-98, p. 83.

¹⁷¹ For their adoption, the European Commission is not obliged to ask for an EDPS’ opinion, and the EDPB is consulted by virtue of Article 70(1)(s) GDPR read in conjunction with Article 42(4) EUDPR. The EDPB complains about not having been forwarded the relevant documentation on time to issue a prompt opinion in, among others, the Recommendations of the EDPB No. 01/2021 on *the adequacy referential under the Law Enforcement Directive*, Brussels, 2.02.2021, p. 5.

¹⁷² Christopher Kuner, “Article 45: Transfers on the basis of an adequacy decision”, in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *op. cit.*, pp. 771-766, p. 775.

¹⁷³ Articles 35 and 36 and recital (66) LED.

¹⁷⁴ Recent contributions have been made by: Cinzia Peraro, “Protezione extraterritoriale dei diritti: il trasferimento dei dati personali dall’Unione Europea verso Paesi terzi”, *Rivista Ordine Internazionale e Diritti Umani*, No. 3, 2021, pp. 666-691, and Itziar Sobrino García, “Las decisiones de adecuación en las transferencias internacionales de datos. el caso del flujo de datos entre la Unión Europea y Estados Unidos”, *Revista de Derecho Comunitario Europeo*, No. 68, 2021, pp. 227-256.

*Schrems v Data Protection Commissioner*¹⁷⁵, the applicant challenged the Commission Decision 2000/520/EC of 26 July 2000¹⁷⁶ which assessed the adequacy of the protection provided by the Safe Harbour Privacy principles¹⁷⁷ and the related, and frequently asked, questions issued by the US Department of Commerce. The case originated from the refusal of the Irish Data Protection Commissioner to investigate the adequacy of the data protection level in the US following the fact that Facebook Ireland transferred the information from Ireland to Facebook Inc. (US) where the data was finally stored. Specifically, Mr. Schrems alleged that in light of Edward Snowden's exposure of the US' trawling of personal data, the indiscriminate and generalised access to personal data by the National Security Agency was not compatible with EU standards. On the validity of the Commission Decision 2000/520/EC of 26 July 2000, the CJEU recalled that the DPD did not elucidate the meaning of "adequate level of protection", yet it offered some examples in order to assess this circumstance. While referring to Advocate General Bot's Opinion¹⁷⁸, the CJEU affirmed that the decision aimed at preserving the same level of protection beyond the Member States' physical borders:

[...] the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter¹⁷⁹.

The judgment also emphasised that the European Commission's discretion in evaluating the adequacy of the third country's law must be interpreted restrictively and, in any case, that the European Commission itself is called to revise its assessment periodically¹⁸⁰. After the invalidation of the Safe Harbour Privacy Principles, because the principle of strict necessity had been breached, the European Commission adopted another adequacy decision: the EU-US

¹⁷⁵ C-362/14, *Maximillian Schrems v Data Protection Commissioner*.

¹⁷⁶ Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance), *OJ* 2000 L 215, p. 7.

¹⁷⁷ The Article 29 DPWP had been sceptical from the very beginning of their negotiations. See, among others, the following documents: Opinion No. 1/99 on *the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government*, Brussels, 26.01.1999; Opinion No. 2/99 on *the Adequacy of the "International Safe Harbor Principles" issued by the US Department of Commerce*, Brussels, 19.04.1999; Working document on *the current state of play of the ongoing discussions between the European Commission and the United States Government concerning the "International Safe Harbor Principles"*, Brussels, 7.09.1999, and Opinion No. 4/2000 on *the level of protection provided by the "Safe Harbor Principles"*, Brussels, 16.05.2000.

¹⁷⁸ Opinion of Advocate General Bot, C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 23 September 2015, EU:C:2015:627.

¹⁷⁹ C-362/14, *Maximillian Schrems v Data Protection Commissioner*, para 73.

¹⁸⁰ Which is now incorporated in the EU legislation, see Articles 45(4) GDPR and 36(4) LED.

Privacy Shield Act¹⁸¹ that was subject of a new appeal, *Data Protection Commissioner v Facebook Ireland Ltd. and Maximillian Schrems*¹⁸². The preliminary questions were once again provoked by Mr. Schrems' request to suspend or prohibit the transfer of data from Facebook Ireland to Facebook Inc. since the invalidation of the Safe Harbour Principles gave him back the right to put his request before the Irish Court. The CJEU found that unless the EU-US Privacy Shield Act was found to be invalid, national supervisory authorities could not adopt measures contrary to that decision and, consequently, suspend, or end the flow of data toward the US¹⁸³. Nevertheless, contrary to the European Commission's finding, the CJEU rebutted the adequacy of the US legislation on the access to personal data transferred under that Privacy Shield Act as well as the existence of appropriate guarantees regarding the use of data by foreign public authorities for purposes of national security, law enforcement, and public interest. The CJEU specified that these provisions do not prevent supervisory authorities from suspending the transfer of personal data to third countries and international organisations, even though an adequacy decision is in place, '[...] when a complaint is lodged by a person concerning the protection of his or her rights and freedoms in regard to the processing of personal data relating to him or her, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the GDPR and, where relevant, to bring an action before the national courts in order for them, if they share the doubts of that supervisory authority as to the validity of the Commission adequacy decision, to make a reference for a preliminary ruling for the purpose of examining its validity'¹⁸⁴. Indeed, if an adequacy decision had been issued, specific clauses would have empowered the European Commission to repeal, amend, or suspend it¹⁸⁵, as well as to monitor the evolution of the regulation in place in the third country, territory, sector, or international organisation¹⁸⁶.

The *Schrems* saga pushed the European Commission to pay increasing attention to the assessment it conducts for the adoption of adequacy decisions¹⁸⁷, as is the case regarding the

¹⁸¹ Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance) C/2016/4176, *OJ L* 207, 1.8.2016, pp. 1-112.

¹⁸² C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd. and Maximillian Schrems*.

¹⁸³ *Ibid.*, para. 118.

¹⁸⁴ *Ibid.*, para. 120.

¹⁸⁵ See Articles 45(5) GDPR and 51(1)(g) LED.

¹⁸⁶ Articles 45(4) GDPR and 36(4) LED.

¹⁸⁷ Article 50 GDPR depicts the European Commission and national supervisory authorities as ambassadors of the EU data protection standards worldwide. As Christopher Kuner, "Article 50: International cooperation for the protection of personal data", in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *op. cit.*, pp. 858-859, points out that: 'The growth of data protection law and the influence of EU law make it necessary for the EU to interact with other data protection system, both politically and legally. This can include measures such as discussions between regulations and public authorities, bilateral agreements, participation by the EU in

one adopted in relation to Japan in 2019¹⁸⁸ and with the Republic of Korea in 2021¹⁸⁹. These decisions show that, under the recommendation of the EDPB¹⁹⁰, the analysis goes far beyond the assessment of the data protection regime in place in the third country – e.g., the ratification of Convention 108 that proves the EU’s commitment to multilateralism¹⁹¹ – and encompasses a whole comprehensive evaluation of the legal order in place, including existing international commitments or those under negotiation¹⁹². Prof. Kuner underlines that “adequacy” has a different legal quality than other data protection principles:

‘The rationale behind the adequacy concept is the desire to maintain a high level of data protection throughout the EU by preventing circumvention of EU rules through the transfer of processing to third countries with a lower standard of data protection. As such, the

international organizations, and others’. See also Michele Nino, “La sentenza Schrems II della Corte di Giustizia UE: trasmissione dei dati personali dell’Unione europea agli Stati terzi e tutela dei diritti dell’uomo”, *Diritti Umani e Diritto Internazionale* 2020, Vol. 14, No. 3, pp. 733-760; Paul Roth, “Adequate Level of Data Protection in Third Countries Post-Schrems and under the General Data Protection Regulation”, *Journal of Law, Information and Science*, Vol. 25, No. 1, 2017, pp. 49-69, and Gabe Maldoff, Omer Tene, “Essential Equivalence and European Adequacy after Schrems: The Canadian Example”, *Wisconsin International Law Journal*, Vol. 34, 2016, pp. 211-283.

¹⁸⁸ See the Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information (Text with EEA relevance) C/2019/304/, *OJ L* 76, 19.3.2019, pp. 1-58, commented by Juan José Gonzalo Domenech, “Las decisiones de adecuación en el Derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los estados miembros”, *Cuadernos de Derecho Transnacional*, No. 1, Vol. 11, 2019, pp. 350-371. The EU strategy on the choice of the partners with which undertake the adequacy evaluation see the Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World, COM(2017) 7 final, Brussels, 10.1.2017. The lists of adequacy decisions adopted by the European Commission is available in its official webpage at www.ec.europa.eu.

¹⁸⁹ Commission implementing decision of 17.12.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act, C(2021) 9316 final, Brussels, 17.12.2021, and the Opinion of the EDPB No. 32/2021 on the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/769 on the adequate protection of personal data in the Republic of Korea. Version 1.0, Brussels, 24.09.2021.

¹⁹⁰ Article 70(1)(s) GDPR.

¹⁹¹ On 3 March 2021 the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions empty, 2030 Digital Compass: the European way for the Digital Decade, COM(2021) 118 final, Brussels, 9.3.2021, called for the collaboration of international partners to pave the way toward a Digital Transformation for the 2020-2030 decade – which has been discussed extensively under the ‘Digital Compass’ tag.

¹⁹² Article 45(2)(c) GDPR and 36(2) LED. Provided that Article 44 GDPR requires to assess the possibility of onward transfer of personal data – i.e., ‘further transfer of personal data after they have been transferred to a data importer outside the EU or EEA’ in Christopher Kuner, 2020, “Article 44: General Principles for transfer”, *op. cit.*, p. 763 – it is understandable that the European Commission is called to assess the eventually transfer of data to third countries and organisations at the macro and micro levels. This is perfectly aligned with the so-called Brussels effect for which as far as third actors applies EU rules in their own international relations, the EU external action goes far beyond its international commitment. See Joanne Scott, “The Global Reach of EU Law”, in Marise Cremona and Joanne Scott, *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, Oxford, Oxford University Press, 2019, pp. 21-63.

concept serves a political end (preventing circumvention of EU law), rather than being a principle of data processing in itself¹⁹³.

According to the EDPS: ‘Adequacy does not require adopting a framework which is identical to the one existing in the EU, but, taken as whole, the [foreign] legal order should cover all the key elements of the EU data protection framework’¹⁹⁴. In reality, the purpose is to assess not only that data protection rules are established in accordance with the EU primary law¹⁹⁵, but also that the individual is guaranteed procedural means that provide for the effectiveness of the foreign law¹⁹⁶. Articles 45(2)(a) GDPR and 36(2) LED establish that the following elements shall be taken into account, *inter alia*:

- the rule of law;
- the respect for human rights and fundamental freedoms;
- any relevant legislation, both general and sectoral, including that concerning public security, defence, national security and criminal law¹⁹⁷, and the access of public authorities to personal data, as well as the implementation of such legislation¹⁹⁸;
- data protection rules;

¹⁹³ Christopher Kuner, “Developing an Adequate Legal Framework for International Data Transfers”, in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, and Sjaak Nouwt, *Reinventing Data Protection?*, Luxembourg, Springer, 2009, pp. 263-274, pp. 266-267.

¹⁹⁴ Opinion of the EDPS No. 4/2016 on *the EU-U.S. Privacy Shield draft adequacy decision*, Brussels, 30.05.2016, p. 6.

¹⁹⁵ Stefano Saluzzo, “The EU as a Global Standard Setting Actor: The Case of Data Transfers to Third Countries”, in Elena Carpanelli and Nicole Lazzerini, *Use and Misuse of New Technologies: Contemporary Challenges in International and European Law*, Switzerland, Springer, 2019, pp. 115-134.

¹⁹⁶ See the Discussion Document of the Article 29 DPWP, *First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy*, Brussels, 26.06.1997, p. 4, that concretises these procedural aspects in the provision of liabilities, sanctions, remedies, supervisory authorities, and notification.

¹⁹⁷ At this proposal, the – see the Article 29 DPWP, *Adequacy Referential*, Brussels, 6.02.2018, *in fine*, suggests taking into account four main features in the field of surveillance, namely: the fact that the processing should be based on clear, precise and accessible rules (legal basis); the principles of necessity and proportionality with regards to legitimate objectives pursued need to be demonstrated; the necessity to ensure that processing has to be subject to independent oversight, and existence of effective remedies available to the individual.

¹⁹⁸ It is important here to recall the CJEU jurisprudence on the retention of personal data and the applicable “strict necessity” test analysed in the previous Chapter to which the European Commission will have to pay special attention. See also the Recommendations of the EDPB No. 02/2020 on *the European Essential Guarantees for surveillance measures*, Brussels, 10.11.2020.

- professional rules and security measures¹⁹⁹, including rules for the onward transfer of personal data to another third country or international organisation which must be complied with in that country or international organisation²⁰⁰;
- case-law, as well as effective and enforceable data subject rights, and
- effective administrative and judicial redress for data subjects whose personal data are being transferred²⁰¹.

Furthermore, the European Commission shall consider whether an independent supervisory authority with enforcement powers in charge of informing the individuals on their subjective data protection rights is in place in the third country²⁰². All in all, the dialogue that the European Commission undertakes to adopt an adequacy decision enables it not only to outsource its data protection principles, but also to promote the EU's value and principles among which fundamental rights stand out²⁰³. As the Article 29 DPWP highlights:

‘Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules. [...] It is therefore clear that any meaningful analysis of adequate protection must comprise the two basic elements: the content of the rules applicable and the means for ensuring their effective application. It is upon the European Commission to verify – on a regular basis – that the rules in place are effective in practice’²⁰⁴.

However, these merits do not shelter adequacy decisions from criticism. The comprehensive assessment conducted by the European Commission to adopt an adequacy decision puts into question the effectiveness and efficiency of this instrument, as its adoption is time-consuming

¹⁹⁹ See the EDPB, “Thirty-second plenary session: Statement on the interoperability of contact tracing applications, statement on the opening of borders and data protection rights, response letters to MEP Körner on laptop camera covers and encryption and letter to the Commission”, *Press Release*, Brussels, 17.06.2020, where it recalled that the existence of encryption bans in third countries ‘seriously undermine compliance with GDPR security obligations applicable to controllers and processors’ and shall be taken into account by the European Commission before issuing an adequacy decision.

²⁰⁰ For example, Germany quoted the Asia-Pacific Economic Cooperation and Economic Community of West African States as “young” international organisations provided of an international data protection system – see the Council of the EU, 6723/5/13 REV5, Brussels, 12 December 2013, p. 27. In Clare Sullivan, “EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era”, *Computer Law & Security Review*, No. 35, 2019, pp. 380-397, a comparison between the GDPR and the Asia-Pacific Economic Cooperation and Economic Community regime on data transfer can be found. The author comes to the conclusion that the GDPR is better positioned to regulate Internet of Things (IoT) operations while ensuring a high level of protection of individuals fundamental rights.

²⁰¹ See the document of the Discussion Document of the Article 29 DPWP, *First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy*, Brussels, 26.06.1997, p. 8. On that time, it was estimated that Convention 108 constituted a good starting point in order to legitimate the transfer of personal data to third countries, yet two lacunas should have been filled in: firstly, the provision of an independent supervisory authority with appropriate powers (especially investigative power) and, secondly, the third country in question should have been the final destination of the transfer and not an intermediary country.

²⁰² Article 45(2)(b) GDPR.

²⁰³ See Article 3(5) TEU, and “Les États membres de l'UE s'engagent avec leurs partenaires de la zone indo-pacifique pour promouvoir la protection des données”, *Bulletin Quotidien Europe*, No. 12899, 26.2.2022.

²⁰⁴ Article 29 DPWP, *Adequacy Referential*, Brussels, 6.02.2018, and also the Recommendations of the EDPB No. 01/2021 on the adequacy referential under the Law Enforcement Directive, Brussels, 2.02.2021, p. 5.

and expensive, without ensuring the enforceability of EU standards by third partners²⁰⁵. According to Prof. Kuner, the adequacy decision represents another manifestation of EU extraterritorial jurisdiction established on the basis of a connection rule consisting of the protection of EU residents and citizens or, even more stringently, in ‘the processing of personal data of State’s own nationals and residents’²⁰⁶. Specifically, EU unilateral action has been attacked for ‘imperial’ outsourcing continental standards while causing political tensions in cases where the diplomatic dialogue is not followed by the adoption of any decision²⁰⁷. During the negotiations of the new data protection package, the European Commission’s competence and legitimacy in adopting adequacy decisions were strongly questioned by the United Kingdom, which looked upon the assessment conducted of a third country’s foreign legislation, national security provisions and international commitments with suspicion²⁰⁸. Nevertheless, a judgment from the United Kingdom may not be reliable if it is considered that this country is one of the closest allies of the US²⁰⁹.

Provided that decisions adopted under the GDPR are not valid for LED purposes and vice versa – which is confirmed by the EUDPR’s wording that refers to both instruments²¹⁰ – so far,

²⁰⁵ Christopher Kuner, 2009, *op. cit.*, p. 263 ff., and Christopher Kuner, “Reality and Illusion in EU Data Transfer Regulation Post Schrems”, in *German Law Journal*, Vol. 18, No. 4, 2017, pp. 881-918.

²⁰⁶ Christopher Kuner, 2013, *op. cit.*, p. 125. Of the same opinion are Cedric Ryngaert and Mistale Taylor, “The GDPR as Global Data Protection Regulation?”, *American Journal of International Law Unbound*, Vol. 114, 2020, pp. 5-9.

²⁰⁷ Christopher Kuner, 2013, *op. cit.*, p. 66.

²⁰⁸ See the Council of the EU, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Comments on Chapter*, 6723/5/13 REV5, 12 December 2013, p. 136.

²⁰⁹ See Chapter I.

²¹⁰ Article 47 EUDPR and Laura Drechsler, “Comparing LED and GDPR Adequacy: One Standard Two Systems”, *Global Privacy Law Review*, Vol. 1, No. 2, 2020, pp. 93-103. The interpretation given by the CJEU on the first/third pillar dichotomy analysed in Chapter I impacts the adoption of adequacy decisions under the GDPR or the LED respectively. In this sense, the access of law enforcement authorities and intelligent services to personal data stored by private companies for other purposes – e.g., commercial ones – seems to be backed up by an adequacy decision stemming from the GDPR and not the LED. In C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, para. 87, the referring judged asked the CJEU whether it fell within EU law the transfer of data from Facebook Ireland to Facebook Inc. for commercial purposes under the Standard Contractual Clause validated by a European Commission’s Decision, even when the third country processed the data disclosed for national security and law enforcement purposes, as well as to conduct foreign affairs. The CJEU answered positively to this question, by stating that it falls within the scope of the GDPR the international transfer of data for commercial purposes between two legal persons, even when at the time of transfer or thereafter, the data is processed by the authorities of the third country in question for public security, defense, and state’s security purposes. This circumstance does not jeopardise the fact that the underlying adequacy decision was based on the GDPR. Indeed, the CJEU highlighted that through its adequacy decision the European Commission evaluates, among other, the legislation of the third country on public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation. The result is different, instead, when private entities are “delegated” the exercise of public functions for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security according to Article 3(7)(b) of the LED.

the European Commission has adopted fourteen adequacy decisions based on the GDPR²¹¹, and one adequacy decision based on the LED, relating to the United Kingdom²¹². The GDPR and the LED²¹³ clarify that adequacy decisions can acquire different scopes of application to ensure the transfer of data toward a third country, a territory, or specified sectors within a third country²¹⁴ including, among others, those within the IT domain. In this sense, Prof. Kuner finds other examples of adequacy in the PNR agreements concluded by the EU²¹⁵ and the TFTP agreement concluded between the EU and the US²¹⁶. Indeed, when the Privacy Shield act was invalidated, the CJEU affirmed that that no legislative vacuum was created following its judgment since other appropriate safeguards could be adopted concerning the transfer data from the EU to the US based on the GDPR dispositions²¹⁷. This reasoning seems to have been embraced by the CJEU too, in *Opinion 1/15* with regard to the draft EU-Canada PNR Agreement²¹⁸. However, sticking to the GDPR and the LED provisions, we believe that these

²¹¹ Consult the European Commission's official webpage at www.ec.europa.eu.

²¹² See the Commission implementing decision pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, C(2021) 4801 final, Brussels, 28 June 2021, announced in "Adéquation du régime britannique de protection des données personnelles, le PE demande à la Commission de revoir sa copie", *Bulletin Quotidien Europe*, No. 12724, 22.05.2021. See also the Recommendations of the EDPB No. 01/2021 on the adequacy referential under the Law Enforcement Directive, Brussels, 2.02.2021.

²¹³ Indeed, the adequacy decision is regulated in the same way in both instruments with the sole difference that the LED is targeted at the Member States, and it misses a paragraph (9) referring to the European Commission's implementing decisions adopted previous to the LED's entry into force.

²¹⁴ Article 45(1) GDPR and Article 36(3) LED.

²¹⁵ Council Decision 2012/381/EU of 13 December 2011 on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, *OJ L* 186, 14.7.2012, p. 3; Council Decision 2006/230/EC of 18 July 2005 on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of API/PNR data Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data, *OJ L* 82, 21.3.2006, pp. 14-19, and Council Decision 2012/472/EU of 26 April 2012 on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, *OJ L* 82, 21.3.2006, pp. 14-19.

²¹⁶ Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, *OJ L* 8, 13.1.2010, pp. 11-16.

²¹⁷ Article 45(7) GDPR:

‘A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49’,

and Article 36(7) LED:

‘Member States shall provide for a decision pursuant to paragraph 5 to be without prejudice to transfers of personal data to the third country, the territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 37 and 38’.

²¹⁸ See *Opinion 1/15*, para. 214:

‘In those circumstances, such disclosure requires the existence of either an agreement between the European Union and the non-member country concerned equivalent to that agreement, or a decision of the Commission,

international agreements really fall within the category of “appropriate safeguards”²¹⁹ and not within that of “adequacy decisions”. If so, adequacy decisions and international treaties remain two different channels for protecting and transferring personal data that are correlated by an alternative hierarchical relationship as further analysed below²²⁰.

2.1.2. The relationship between adequacy decisions and international agreements in the data protection field

The conclusion of an international agreement allows the transfer personal data in the absence of an adequacy decision and its use is preferable over derogation clauses²²¹. According to Prof. Kuner: ‘[a]ny conflicts between these three types of mechanism should be resolved with this hierarchy in mind, and with the aim to maximize the level of data protection for the transfer’²²². Specifically, international agreements as means to facilitate transfer are categorised under the label of ‘legally binding and enforceable instrument between public authorities or bodies’ in the GDPR²²³ and as ‘legally binding instrument[s]’ in the LED, respectively²²⁴. The author notes that the choice of an adequacy decision or an international agreement ‘depends on a variety of factors, both legal and political’²²⁵:

‘[...] Changes to the law have also made it easier to adopt adequacy decision for data sharing; for example, the Commission may now also issue such decisions under the LED. The Commission has determined that data transfer in the context of international trade are to be legalized by adequacy decisions rather than by international agreements. However, the legal relationship between international agreements and adequacy decisions remains confused, as illustrated by the so-called Umbrella Agreement between the EU and the US dealing with the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences. While stating that on the one hand it does not provide a legal basis for data transfers, the Umbrella Agreement also proclaims that data processing under it shall be deemed to comply with laws restricting the international transfer of data, which makes it sound like an adequacy decision [...]’²²⁶.

Therefore, the former would be usually preferred as it is easier to adopt. Such an interpretation raises concerns of legal certainty *vis-à-vis* the EU regime on the protection and

under Article 25(6) of Directive 95/46, finding that the third country ensures an adequate level of protection within the meaning of EU law and covering the authorities to which it is intended PNR data be transferred’.

²¹⁹ See Article 46(2) and (3) GDPR, as well as Articles 36 and 37 LED.

²²⁰ In a more synthetic way, see Francesca Tassinari, “The European Union Adequacy Standard in the Field of Data Protection: A Competence Approach”, *Diritti Umani e Diritto Internazionale*, No. 1, Vol. 16, 2022, pp. 5-38.

²²¹ Article 49 GDPR and Article 38 LED.

²²² See Christopher Kuner, 2020, “Article 44: General Principle for transfer”, *op. cit.*, p. 765.

²²³ Article 46(2)(a) GDPR.

²²⁴ Article 37(1)(b) LED.

²²⁵ See Christopher Kuner, 2020, “Article 45: Transfers on the basis of an adequacy decision”, *op. cit.*, p. 777.

²²⁶ *Ibidem*.

transfer of personal data and, as a last resort, leaves unresolved the question on whether, and how the EU, is entitled to exercise its external competence based on Article 16 TFEU.

The use of one or other legal basis is of crucial importance if it is considered that, unlike adequacy decisions, ‘[appropriate] safeguards under the Directive and the GDPR are to be understood as data protection guarantees which do not already exist in the legal system of the country to which the data are to be transferred and are created for specific data transfer situations’²²⁷. Also, the CJEU has started tracing a dividing line between one tool and the other. When evaluating the standard contractual clauses validated by the Commission’s Implementing Decision (EU) 2016/2297 of 16 December 2016²²⁸, the CJEU maintained that these clauses should have ensured appropriate safeguards, enforceable rights, and effective legal remedies by taking into account not only the contractual clauses agreed, but also any access by the public authorities of that third country to the personal data transferred and the relevant aspects of the legal system of the third country. In this sense, the CJEU recalled that the third country’s legislation should have been assessed on the basis of Article 45(2) GDPR. Standard contractual clauses recall the US self-regulatory model, already incorporated in the DPD²²⁹, which binds controllers established in the EU and the recipient of data based in a third country only when the latter decides to insert those clauses into a contract. Consequently, and unlike cases in which an adequacy decision exists, when the transfer of personal data is carried out by virtue of the existence of appropriate safeguards, it is up to the data protection controller or processor to assess the existence of a level of protection essentially equivalent to that of the EU and, in particular, that the data subject is granted enforceable rights and judicial remedies²³⁰. In this respect, the European Commission’s intervention is limited to the approval of standard contractual clauses, without being obliged to conduct a general assessment of the third country’s

²²⁷ Christopher Kuner, 2015, *op. cit.*, p. 237.

²²⁸ See the Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2016) 8471) (Text with EEA relevance), C/2016/8471, OJL 344, 17.12.2016, pp. 100-101.

²²⁹ Previous Article 26(1) and (4) DPD, today’s Article 46(2)(c) and (d) GDPR. According to the new GDPR, standard contractual clauses can be adopted by the European Commission or approved by it on the basis of the ones proposed by a supervisory authority. Note that Article 62(3) GDPR specifies that, under approval of the competent supervisory authority, the appropriate safeguards of Article 46(2) GDPR can consist of contractual clauses between the controller or processor and the controller, processor or recipient of the personal data in the third country or international organisation, or provisions to be inserted into administrative arrangements between public authorities or bodies, and which include enforceable and effective data subject rights.

²³⁰ The Recommendations of the EDPB No. 01/2020 on *measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data: Version 2.0*, Brussels, 18.06.2021, provides a set of criteria on which each data controller could base their assessment.

national law on the protection of personal data. Therefore, the CJEU found that the transfer of data might require the adoption of supplementary measures when standard contractual clauses are agreed as well²³¹. If these supplementary measures cannot be adopted, even though they are needed to safeguard the adequate level of protection, then data controllers and processors must suspend or end the transfer toward third countries²³². From the CJEU's position, it is clear that the lack of a decision on adequacy cannot be replaced *sic et simpliciter* by the adoption of appropriate safeguards, under which international agreements are a notable example. Conversely, this type of instrument requires additional safeguards for the lawful transfer of personal data.

The Article 29 DPWP has repeatedly clarified that “no adequacy” is not a synonym for a “bad country”. Rather, it means that no guidance on that third country's internal legislation on data protection is available²³³. In this sense, adequacy decisions are put in place to fill any legal gaps. Nevertheless, practice shows that they are not used in this manner. Again, the US example is significant to elucidate the adequacy decision's relationship with international treaties because of its divergent legislation on personal data, which led the CJEU to rule against the US

²³¹ It follows that the standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the EU and, consequently, independently of the level of protection guaranteed in each third country. In so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection, in C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd, and Maximillian Schrems*, para. 133.

²³² In any case, the EU-US Standard Contractual Clauses Decision was finally found to be compatible with the CFREU as it ensures an effective mechanism to suspend or prohibit the transfer of data to third countries where the recipient of the data does not comply with the clauses or cannot do it. See CJEU, *ibid.*, paras. 141-147, where the CJEU found that the evaluation on compliance with standards by recipients should be assessed on a case-by-case basis so that the processing activity developed within the third country could not go beyond what is necessary in a democratic society, also to achieve national security, defence and public security. On the one hand, the recipient is required to communicate to EU controllers or processors the existence of any inability to comply with those clauses, in which case the data already transferred is to be returned or destroyed while allowing the data subject to receive the appropriate compensation. On the other, the controller or processor in the EU must notify to the data subject that the transfer of data did not comply with an adequate protection, to enable the latter to bring a legal action against the controller or notify the competent national supervisory authority in order to have the transfer of data suspended or prohibited.

²³³ However, this seemed to be the original intention of the European Commission. See Article 40(5) of the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 011 final of 25 January 2012, which would have enabled the European Commission to adopt a “non-adequacy decision”. Several Member States – e.g., France – opposed it because of the diplomatic consequences that a blacklist might have caused. See the Council of the EU, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – Comments on Chapter V*, 6723/13, 26 February 2013, p. 35.

inadequacy on two occasions²³⁴. After the invalidation of the Commission Decision on the adequacy finding and the Council Decision on the conclusion of the EU-US PNR Agreement of 2002, the CJEU stated that ‘[i]n order to achieve a harmonised and consistent EU approach, bilateral agreements between the US and the EU Member States should be avoided’ and it encouraged²³⁵ the adoption of a “transitory agreement” to overcome the legislative gaps following its judgment²³⁶. Thus, the CJEU called on the EU to agree an international treaty before it could offer guidance on its internal legislation, though this was found to be inadequate according to EU standards. The Article 29 DPWP, for its part, recommended concluding a treaty based on Article 16(2) TFEU²³⁷ to resolve the conflict of laws impacting EU private companies when they were asked by foreign authorities to access their servers, or to hand over personal data on a large-scale without the back-up of an adequacy decision²³⁸. Indeed, if the third parties involved did not count on an adequacy decision, the disclosure of personal data by EU companies would infringe EU law, while their refusal to disclose information, or to answer enquiries would expose them to other sanctions²³⁹. Therefore, the Article 29 DPWP confirmed

²³⁴ The differences between the US and EU legal systems as far as personal data is concerned have been well highlighted by Ioanna Tourkochuriti, “The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide between U.S.-EU in Data Privacy Protection”, *University of Arkansas at Little Rock Law Review*, Vol. 36, No. 2, 2014, pp. 161-176, and Alison White, “Control of Transborder Data Flow: Reactions to the European Data Protection Directive”, *International Journal of Law and Information Technology*, Vol. 5, No. 2, 1997, p. 230-247.

²³⁵ Sentencing the inadequacy of the US’ legal order had significant impact on the EU’s digital economy since the tech giant Google, Apple, Facebook, Amazon and Microsoft (GAFAM) threatened not offer their services to EU citizens. Latest claims came from Facebook as reported by Pascale Davies, “Meta warns it may shut Facebook in Europe but EU leaders say life would be ‘very good’ without it”, *euronews.next*, 9.02.2022, available at www.euronews.com.

²³⁶ In these terms, the Article 29 DPWP encouraged the adoption of a global level of traffic air security and the respect of human rights – see its Opinions No. 5/2006 on the ruling by the European Court of Justice of 30 May 2006 in *Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States*, Brussels, 14.06.2006 and No. 04/2014 on *Surveillance of electronic communications for intelligence and national security purposes*, Brussels, 10.04.2014, p. 7.

²³⁷ See the Opinion of the Article 29 DPWP No. 04/2014 on *Surveillance of electronic communications for intelligence and national security purposes*, Brussels, 10.04.2014, p. 8.

²³⁸ Indeed, Edward Snowden revealed that the US National Security Agency was accessing personal data that had been previously transferred from an EU company established in the EU to another company present in the US territories. The Working Document of the Article 29 DPWP on *surveillance of electronic communications for intelligence and national security purposes*, Brussels, 5.12.2014, p. 37, contemplates three different possible scenarios: a direct transfer/direct access from an EU private entity to a non-EU public authority; a transfer from an EU private entity to a non-EU private entity not under EU jurisdiction; and a transfer from one EU establishment to a non-EU establishment under EU jurisdiction.

²³⁹ Today, the disclosure of personal data to foreign authorities by private companies is addressed under Article 48 GDPR and Article 39 LED. The former forbids data controllers and processors to exchange or disclose personal data before a judgment of a court or tribunal, or any decision of an administrative authority of a third country. Indeed, these requests are to be justified by a specific legal basis, such as a mutual legal assistance agreement – see also recital (67) EUDPR. The latter, instead, provides that Member States may allow national authorities to transfer personal data to “recipients” established in third countries under the aegis of a bilateral or multilateral international agreement in the field of judicial cooperation in criminal matters and police cooperation, or by accomplishing the conditions set forth under its first paragraph. In any case, competent authorities are to inform

that an international agreement was necessary to justify the transfer or disclosure of personal data toward the US²⁴⁰. Interestingly, in 2016, an EU-US Umbrella Agreement was concluded²⁴¹ precisely to overcome the impossibility of adopting an adequacy decision regarding the US. The Agreement is a clear projection of Article 16 TFEU-based LED with fallout in the AFSJ²⁴², though discrepancies between the Agreement and the LED are visible²⁴³. Another agreement of principles on a new transatlantic data protection framework based on the GDPR was announced on 25 March 2022²⁴⁴, but the text had not been published yet at the time of closing our research.

The EU-US Umbrella Agreement seeks to '[...] ensure a high level of protection of personal information and enhance cooperation between the United States and the European Union and its Member States, in relation to the prevention, investigation, detection or prosecution of criminal offences, including terrorism'²⁴⁵ for which purpose it establishes standards of protection on the transfer of personal data between competent authorities established in the US

their national supervisory authority and in the case of a transfer based on Article 39(1) LED, this has to be documented – see recital (73) LED and the Opinion of the Article 29 DPWP No. 01/2012 on *the data protection reform proposals*, Brussels, 23.03.2012, p. 23. Remarkably, the issue of extraterritorial impositions on EU Member States was already raised by the Article 29 DPWP because common and civil jurisdictions regulate differently the exchange of information in the pre-trial phase – see the Working Document of the Article 29 DPWP No. 1/2009 on *pre-trial discovery for cross border civil litigation*, Brussels, 11.02.2009, pointing out that, among different options available, the transfer of information should have been based as far as possible on the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, signed in the Netherlands, 18 March 1970, entered into force on 7 October 1972, available at www.hcch.net.

²⁴⁰ Specifically, the Article 29 DPWP Opinion No. 04/2014 on *Surveillance of electronic communications for intelligence and national security purposes*, Brussels, 10.04.2014, p. 15, underlines that third countries' public authorities should have direct access to private sector servers falling under the scope of the DPD and that, in any case, the transfer had to be justified by virtue of an international agreement between the Member State and a third country. The agreement should have provided for appropriate safeguards, which is not the case when it is kept secretly.

²⁴¹ Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences. On the EU-US relationship on the transfer of personal data, including the Umbrella Agreement, see Cristina Blasi Casagran, *op. cit.*, pp. 100-111.

²⁴² See Article 27 of the EU-US Umbrella Agreement, which provides for a special attention toward Denmark, the United Kingdom, and Ireland as these countries have been granted rights to opt into the Agreement according to Protocol No 21. On variable geometry, see Chapter I.

²⁴³ See the Opinion of the EDPS on *the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection*, Brussels, 6.06.2009, para. 35.

²⁴⁴ See, for example, Vincent Manancourt, "EU, US strike preliminary deal to unlock transatlantic data flows", *POLITICO*, 25.03.2022, available at www.politico.eu. This GDPR-based agreement is expected to regulate the transfer of personal data between the EU and the US so as to fill the gaps provoked by the Schrems judgments. Following the conclusion of the agreement, Washington is expected to adopt a decree that the European Commission will be used for a 'potential' future decision on adequacy according to "Transfert et protection des données, la Commission annonce un accord de principe sur un nouveau cadre avec les États-Unis", *Bulletin Quotidien Europe*, No. 12919, 26.3.2022.

²⁴⁵ Article 1(1) of the EU-US Umbrella Agreement. This excludes the possibility that the Umbrella Agreement is a soft law measure, but not that it provides for 'soft provisions'.

and the EU respectively²⁴⁶. Prof. Kuner notes that this Agreement sits in a grey area between adequacy decisions and appropriate safeguards. The author highlights that the EU-US Umbrella Agreement should not provide a legal basis to transfer personal data, since it cannot – at least not fully – be considered an appropriate safeguard. Despite this, he notes that the data processing activities falling under the agreement ‘shall be deemed to comply with laws restricting the international transfer of data’ and, consequently, the agreement seems to be upgrading itself to the adequacy decision level²⁴⁷. We believe that a competence approach may help to shed light on the EU-US Umbrella Agreement’s position.

Assuming that a ‘legally binding (enforceable) instrument’ should never be considered a surrogate for the lack of an adequacy decision in the terms set out above, the possibility that the EU-US Umbrella Agreement constitutes a valid legal basis for transfer has to be assessed *vis-à-vis* the “enforceability” standard that, it should not be forgotten, is expressly required under Article 45(2)(a) GDPR, but not under Article 37(1)(a) LED. In the absence of any CJEU pronouncement, it is not clear whether such a contradiction is significant or not²⁴⁸: if the incongruity is significant, we believe that the EU-US Umbrella Agreement should be deemed a valid legal basis to transfer personal data. However, taking an approach that offers the strongest guarantee leads us to maintain that the EU-US Umbrella Agreement should not be deemed a valid legal basis – i.e., it is not enforceable²⁴⁹. The EU-US Umbrella Agreement is a framework treaty whose norms are expected to supplement the provisions on the protection of personal data inserted into other EU-US treaties²⁵⁰. This implies, among other things, that envisaged agreements should further specify the terms under which the protection of transferred data is ensured²⁵¹. Had the EU wanted to use it not only to enhance the US data protection

²⁴⁶ Article 1(3) of the EU-US Umbrella Agreement.

²⁴⁷ Christopher Kuner, 2020, “Article 45: Transfers on the basis of an adequacy decision”, *op. cit.*, p. 777.

²⁴⁸ Compare the Opinion of the EDPB No. 1/2022 on *the two Proposals for Council Decision authorizing Member States to sign and ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, Brussels, 20.01.2022, with the Letter of the Chair of the EDPB to Chairman of the Committee on Civil Liberties, Justice and Home Affairs, Brussels, 22.03.2022: while the former finds that the Second Additional Protocol to the Budapest Convention is legal binding (p. 6), the latter highlights that it is a ‘legally binding and enforceable instrument’ (p. 2).

²⁴⁹ See recital (71) LED:

‘Such legally binding instruments could, for example, be legally binding bilateral agreements which have been concluded by the Member States and implemented in their legal order and which could be enforced by their data subjects, ensuring compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress’.

See also the Consultation of the EDPS on *the future EU-US international agreement on personal data protection and information sharing for law enforcement purposes*, Brussels, 12.03.2013.

²⁵⁰ Article 5(1) of the EU-US Umbrella Agreement.

²⁵¹ According to Teresa Fajardo del Castillo, “El acuerdo de París sobre el cambio climático: sus aportaciones al desarrollo progresivo del derecho internacional y las consecuencias de la retirada de los Estados Unidos”, *Revista*

legislation, but also as a valid legal basis to transfer personal data, then the EU-US Umbrella Agreement would have needed to meet the “legally binding enforceability” requisite²⁵². This is what the EU tried to do with the latest draft EU-Canada PNR Agreement that gathered both the protective and the transfer sides, but the CJEU rejected the European Commission’s initiative. However, it is precisely this second hypothesis that raises further criticism. From a competence perspective, the EU-US Umbrella Agreement and the draft EU-Canada PNR Agreement differ according to their legal bases.

The EU-US Umbrella Agreement and the draft EU-Canada PNR Agreement rely on Article 16 TFEU as the correct legal basis that confers on the EU the competence to conclude the agreement, but only the former is genuinely based on Article 16 TFEU. Provided that its adoption followed a “negative opinion” on adequacy, it is here suggested that the exercise of the EU external (implied) competence based on Article 16 TFEU is unusually pre-empted if an adequacy decision exists. In these terms, adequacy decisions represent another (privileged) means of exercising the EU external (implied) competence based on Article 16(2) TFEU, instead of its treaty-making power. Indeed, in case the former is invalidated, the transfer of personal data can be channelled through appropriate safeguards, including legally binding (and enforceable) instruments, or derogation clauses. Zinser finds that in case of non-adequacy or, even better, in case of a negative assessment on adequacy: ‘[...] the European Commission shall enter into negotiations with a view to remedying the situation. The Directive does not describe the method of remedying the situation. However, the aim is clear: the third country in question has to achieve an adequate level of protection’²⁵³. Following the US example, we could infer that this “remedy” takes place through the conclusion of an international agreement setting out the requirements to be met by the third country or international organisation. However, the EU-US Umbrella Agreement is neither deemed to replace the adequacy decisions the CJEU had invalidated²⁵⁴, nor it is framed within Article 46(2)(a) GDPR or 37(1)(a) LED, first and

Española de Derecho Internacional, Vol. 70, No. 1, 2018, pp. 23-51, p. 35: ‘[...] each framework agreement triggers an ongoing negotiating process that informs its future regulatory development and its own institutional structure’ (our own translation).

²⁵² See *infra*.

²⁵³ Alexander Zinser, 2004, *op. cit.*, p. 177.

²⁵⁴ Opinion of the EDPS on *the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection*, Brussels, 6.06.2009, para. 41:

‘The EDPS considers that only a real adequacy test would ensure sufficient guarantees as to the level of protection of personal data. He considers that a general framework agreement with a scope as broad as the one of the HLCG report would have difficulties to pass, as such, a real adequacy test. The adequacy of the general agreement could be acknowledged only if it is combined with an adequacy of specific agreements concluded on a case by case basis’.

foremost because it is not a valid legal basis for transferring personal data. The conclusion of this Agreement can be explained only in the light of the exercise of the EU external (implied) competence based on Article 16 TFEU, which enables the EU to intervene in the external layer so as to ensure the non-circumvention of its internal rules.

Conversely, in the draft EU-Canada PNR agreement, Article 16 TFEU would have been flanking another legal basis, namely Article 87(2)(a) TFEU²⁵⁵. With this draft Agreement, the EU aimed at sealing a cooperative treaty based on the exchange of information, including personal data, rather than equating the other state's level of protection with its own. However, the CJEU's Opinion evaluated both law enforcement and data protection objectives equally. We should recall that with the draft EU-Canada PNR Agreement the EU was (riskily) relying²⁵⁶ on the adequacy decision adopted for Canada in 2005²⁵⁷, on which basis an API/PNR Agreement was concluded the following year²⁵⁸. Indeed, although the Commission Decision 2006/253/EC of 6 September 2005 expired in 2009, the draft Agreement emphasised that '[...] the Canada Border Services Agency unilaterally undertook to assure the EU that the commitments would continue in full force and effect until a new agreement applies'²⁵⁹. Therefore, no sectoral adequacy decision had been adopted as far as the draft EU-Canada PNR Agreement was concerned under the assumption that the third country had kept complying with EU standards. In *Opinion 1/15*, the European Parliament's challenged the fact that the draft EU-Canada PNR Agreement '[sought] to create a form of 'adequacy decision', as provided for in Article 25(6) of [the DPD]'²⁶⁰ by virtue of Article 5 of the draft Agreement. According to it:

'Subject to compliance with this agreement, the Canadian Competent Authority is deemed to provide an adequate level of protection, within the meaning of relevant EU data

²⁵⁵ According to the *Opinion 1/15*, the draft EU-Canada PNR Agreement should have been underpinned by Article 16(2) and Article 87(2)(a) TFEU.

²⁵⁶ It must be noted that the CJEU has been maintaining a wider interpretation of the DPD so as to include third-pillar activities under the first, except for a sole (regretted?) judgment in 2004, that is, cases C-317/04 and C-318/04, *European Parliament v Council of the European Union and Commission of the European Communities*. We are referring to the abundant case law on the Data Retention Directive and the ePrivacy Directive analysed in Chapter I where we highlighted that the CJEU affirmed that both Directives were clearly covered by the DPD. Also, referring to the PNR legislation the Court could make the PNR agreements fall under the GDPR scope instead of the LED scope. This interpretation would explain *a fortiori* the CJEU's willingness in doubly underpinning the draft EU-Canada PNR Agreement with Article 16 and Article 87(2)(a) TFEU, but we cannot take it for granted until the CJEU rules on the matter.

²⁵⁷ *Opinion 1/15*, para. 16, where the CJEU recalled the Commission Decision 2006/253/EC of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency (notified under document number C(2005) 3248) (Text with EEA relevance), *OJ L* 91, 29.3.2006, pp. 49-60.

²⁵⁸ Council Decision 2006/230/EC had not been renovated.

²⁵⁹ Confront the Proposal for a Council Decision on the conclusion of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, COM(2013)0528 final, Brussels, 18.07.2013.

²⁶⁰ *Opinion 1/15*, para. 31.

protection law, for the processing and use of PNR data. An air carrier that provides PNR data to Canada under this Agreement is deemed to comply with EU legal requirements for data transfer from the EU to Canada²⁶¹.

This disposition stated that the Canadian Competent Authority complied with the “adequacy” requirement under the terms of the Agreement while exempting air carriers from any responsibility insofar they met ‘EU legal requirements’. Unfortunately, the CJEU did not spend too many words on the relationship between adequacy decisions and international agreements, but we do not see any reason why these two instruments should be considered as interchangeable. Remarkably, the CJEU recalled that the disclosure of personal data should have not circumvented the level of protection afforded by the EU. This required ‘[...] the existence of either an agreement between the European Union and the non-member country concerned [...], or a decision of the Commission, under Article 25(6) of Directive 95/46, finding that the third country ensures an adequate level of protection within the meaning of EU law [...]’²⁶². Therefore, the adequacy decision/international agreement dichotomy was presented as two alternative options in accordance with the GDPR’s regime on the transfer of personal data. It is true that, and unlike the EU-US Umbrella Agreement, the draft EU-Canada PNR Agreement set down rules on both the protection and the transfer of personal data. However, the CJEU maintained that ‘[...] measures concerning the transfer of personal data to competent authorities in relation to the prevention, detection and investigation of criminal offences and the processing of that data by those same authorities fall within the scope of the police cooperation referred to in Article 87(2)(a) TFEU and may be based on that provision’²⁶³. Thus, the CJEU took into account the “protective” side of Article 16(2) TFEU – i.e., the non-circumvention criterion – and relied upon Article 87(2)(a) TFEU to justify the provisions of the draft EU-Canada PNR Agreement on the transfer of personal data. The possibility of using Article 16(2) TFEU to regulate the free movement of personal data – and, *vis-à-vis* a third country, their transfer – was discarded²⁶⁴, which we find consistent with the objective the Union pursues with its external interventions based on Article 16(2) TFEU.

Now, the legislative choice for which adequacy decisions constitute the first useful tool to protect and exchange personal data is hardly justifiable from a legal perspective if the supranational system of sources is considered. Indeed, the European Commission’ adequacy

²⁶¹ *Ibid.*, Article 5.

²⁶² *Ibid.*, para. 214.

²⁶³ *Ibid.*, para. 99.

²⁶⁴ *Ibid.*, paras. 96 and 104. Besides the CJEU refers to both paragraphs (1) and (2) of Article 16 TFEU which is misleading.

decision is an act of secondary legislation which lies below both EU primary law and secondary law. International agreements, instead, are ‘automatically incorporated into the EU legal order’²⁶⁵ and, specifically, they settle between secondary law and the founding Treaties²⁶⁶. Consequently, if the European Commission adopted an adequacy decision based on the LED, for example, with regard to the US, the hierarchy of tools proposed by the EU data protection *acquis* could not be respected. According to the latter, the EU-US Umbrella Agreement would be somehow “substituted” by the European Commission’s decision, given that the latter provides greater guarantees for individuals and is more effective to accomplish with the non-circumvention goal. However, in terms of public international law, the international agreement would remain valid, unless a specific clause did not take this eventuality into account, which is advisable in our view²⁶⁷. Given this reading, we believe that the co-legislators’ preference for adequacy decisions can be explained in three ways.

First, it can be justified in the light of the principle of subsidiarity, which, in terms of human rights, opts for the regulation on the national level for citizens²⁶⁸. In this regard, adequacy decisions are favoured because they are agreed under the comitology procedure²⁶⁹ where Member State’s delegations can better resist any integrationist push led by the European Commission. As Prof. Hijmans underlines: ‘The Member States are important actors, if only because most data processing takes place within the national jurisdiction, either by authorities of the Member States or by the private sector’²⁷⁰. Second, the provision of a pyramid of instruments for transferring personal data in respect of the data protection *acquis* can be legitimised under the scope of Article 16(2) TFEU. Article 16(2) TFEU is not directed to any kind of transfer or data exchange model, but clearly aims at the establishment of an area of “free

²⁶⁵ Alan Dashwood, Michael Dougan, Barry Rodger, Eleanor Spaventa, and Derrick Wyatt, *op. cit.*, p. 912.

²⁶⁶ Alessandra Gianelli, “Customary International Law in the European Union”, in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *op. cit.*, pp. 93-110, p. 106, highlights that international law enters into the EU legal order through a Council decision that implements the agreement. It is this Council decision that may be invalidated in case the international agreement contrasts with the ‘very fundamental principles’ embedded in EU primary law – where also *ius cogens* norms are contemplated – by virtue of the principle of autonomy of the EU legal order. Conversely, the validity of EU secondary law (not implementing international law) is subjected to EU international obligations, that is the Council decision implementing an international agreement or executing rules of custom nature, being the EU obliged to observe and develop international law, including the principles set forth by the UN Charter – see Article 21(1) TEU.

²⁶⁷ Article 54(a) of the Vienna Convention on the Law of Treaties, signed in Vienna on 23 May 1969, entered into force on 27 January 1980, *U.N.T.S.* Vol. 1155, p. 331

²⁶⁸ Confront Chapter I.

²⁶⁹ Some reflections on the committee procedure regulated under Article 93 GDPR and the adoption of adequacy decisions have been made by Francesca Tassinari, “La adopción de actos delegados y actos de ejecución (comentario a los artículos 92 y 93 del RGPD)”, in Antonio Troncoso Reigada, *Comentario al Reglamento general de protección de datos y la ley orgánica de protección de datos personales y garantía de los derechos digitales*, Pamplona, Thomson Reuters Aranzadi, 2021, pp. 4901-4920.

²⁷⁰ Hielke Hijmans, 2016, *op. cit.*, p. 133.

movement of data”. In our view, this objective infers that the co-legislators have to consider the massive or large-scale movement of data²⁷¹ for which purpose adequacy decisions remain the most suitable instrument to boost intra-Member States exchanges²⁷². Although it is accepted that derogation clauses cannot attain such a goal²⁷³, it is not clear whether, and under what terms, the use of appropriate safeguards can in fact succeed. As a last point of reflection, we believe that preferring adequacy decisions over international agreements is an interesting expedient to, if not circumvent, certainly mitigate the exercise of an EU external (implied) shared competence where the mixed formula risks jeopardising the negotiation of an international treaty on the protection of personal data. However, it is worth analysing the nature of the Union’s (implicit) external competence based on Article 16(2) TFEU before drawing hasty conclusions.

²⁷¹ See the contrary position of the French delegation with regard to the LED in the Council of the EU, *Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data – Chapters V and X*, 6846/14 ADD 1, Brussels, 25 February 2014, pp. 8 and 9, maintaining that:

‘In the absence of an adequacy decision and of a bilateral convention, Member States would run the risk of seeing their diplomatic relations and their operational exchanges with third countries completely destroyed (or, more precisely, suspended until an EU adequacy decision has been adopted), even though many Member States have privileged relations with certain third countries without all the other Member States necessarily having the same kind of relationship. [...] Although the right to obtain effective redress should be one of the factors to be taken into account when assessing whether appropriate safeguards exist for the purposes of allowing data to be transferred to third countries, this criterion must not be an absolute prerequisite for exchanging data with third countries. [...] It is hard to envisage stopping exchanges of this type of data with third countries which are hotbeds of terrorism, as such data is needed in order to prevent attacks on EU territory. Similarly, it is hardly advisable to discontinue mutual legal assistance with third countries which do not offer such means of redress for EU residents, thereby running the risk that individuals who committed crimes on EU territory might flee to those countries to escape prosecution merely because they would have guarantees that their data would not be exchanged’.

²⁷² In this sense, see Santa Slokenberga, “Biobanking and data transfer between the EU and Cape Verde, Mauritius, Morocco, Senegal, and Tunisia: adequacy considerations and Convention 108”, *International Data Privacy Law*, No. 2, Vol. 10, May 2020, pp. 132-145. The author focuses on the exchange of samples in the field of biomedical research and maintains that the adequacy decision is the most valuable tool to share large amounts of personal data as well as to enhance sustainable collaboration and capacity building. Opting for a self-regulatory and proactive responsibility is, instead, Mikel Recuero Linares, “Transferencias internacionales de datos genéticos y datos de salud con fines de investigación”, *Revista de Derecho y Genoma Humano Genética, Biotecnología y Medicina Avanzada*, 2019, pp. 413-433.

²⁷³ The Article 29 DPWP repeatedly underlined that a derogation clause – for example, the one on reasons of public interest – cannot be interpreted as allowing the systematic and massive exchange of information with third countries. See, among others, the Working Document of the Article 29 DPWP on *surveillance of electronic communications for intelligence and national security purposes*, Brussels, 5.12.2014, p. 38 ff. If the data is obtained following a particular inquiry made by a public authority that is issued ‘in accordance with Union or Member State law’, the authority to whom the data is disclosed is not be considered as recipient, yet the processing of personal data must be in compliance with the applicable data protection rules according to the purposes of the processing – Article 4(9) GDPR and recital (64) LED.

2.2. The nature of the European Union's external competence in the field of personal data

2.2.1. The General Data Protection Regulation

With the new GDPR, the EU expressly aims at eliminating any cumulative and simultaneous application of different national laws and to ensure the uniform application of EU law on the assumption that existing practical challenges jeopardise the enforcement of data protection legislation and undermine the co-operation between Member States and their authorities. In this sense, Article 1(2) GDPR states that the Regulation ‘protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data’.

Remarkably, during the negotiations, the European Commission stressed how the lack of common rules would have restricted the cross-border flows of personal data among the Member States if they had maintained different standards. During the negotiation of the new GDPR, Member States fought to lower the provision of binding rules and opted for:

- provisions built upon national law;
- rules that require domestic law to give them effect;
- norms enabling the adoption of more stringent provisions than the ones foreseen by GDPR at the national level, or
- that are even divergent from it²⁷⁴.

Also, as Prof. De Hert notes, ‘[...] the law enforcement system defined by the GDPR and the LED still relies on the intervention of national supervisory authorities. When this turns out to be inadequate it is conceivable one data, based on Article 16 TFEU, to replace this with an enforcement system that relies more on an EU supervisory body’²⁷⁵. As a result, the GDPR appears to be a regulation with a directive's soul, leaving the possibility open for new obstacles to prevent the data flow among the Member States²⁷⁶. In its recital (8), the GDPR establishes that:

‘Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law’.

²⁷⁴ Opinion of the EDPS on *the data protection reform package*, Brussels, 7.03.2012, p. 9.

²⁷⁵ Paul De Hert, 2021, *op. cit.*, p. 297.

²⁷⁶ “Application du RGPD, le manque d'harmonisation entre autorités nationales pointé par les eurodéputés”, *Bulletin Quotidien Europe*, No. 12915, 22.3.2022.

In this sense, the margin of manoeuvre left to the Member States is limited only to the open clauses set forth in the GDPR. Yet, these clauses clearly impede the achievement of full harmonisation in the data protection field²⁷⁷. Conversely, those dispositions that do not leave a margin of manoeuvre to the Member States may be assumed to mark not only the minimum, but also the maximum level of protection granted to individuals²⁷⁸. Remarkably, in *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, the CJEU stressed that the level of protection granted by the GDPR shall be regarded *vis-à-vis* the CFREU only, without taking into account either the ECHR²⁷⁹, or Member States' national law – including their constitutional traditions – in order to ensure the homogeneous application of the rules for the protection of the fundamental rights and freedoms of natural persons whose data is processed within the EU²⁸⁰. In the specific frame of the transfer of personal data to third countries and international organisations, Prof. Kuner maintains that:

‘Member States may not undertake obligations with third countries that affect common rules laid down by the EU, and Member States may act with regard to those areas of shared competences only to the extent that the EU has not done so. Since the GDPR has comprehensive regulated data protection and the rules covering the international data transfers in the Union, in practice, Member States have only limited margin to enter into international agreements governing international data transfer, if all’²⁸¹.

Hence, the author infers that, at least as far as Chapter V of the GDPR is concerned, the EU has regulated to such a large extent that the Member States' treaty-making power is pre-empted even if, for example, it accepts that appropriate safeguards are enumerated under a non-exhaustive list – i.e., no full harmonisation has been achieved. In the same line Prof. Hijmans,

²⁷⁷ Protocol No 25 on the exercise of shared competence, *OJ C* 115, 9.5.2008, p. 307, clarifies that ‘[...] when the Union has taken action in a certain area, the scope of this exercise of competence only covers those elements governed by the Union act in question and therefore does not cover the whole area’ so that even though the EU has exercised its competence, Member States may still find some slots where they are entitled to exercise theirs. See also “Les États membres demandent un réexamen plus large du règlement ‘GDPR’”, *Bulletin Quotidien Europe*, No. 12405, 17.1.2020, according to which: ‘[The Council] also highlights the risk of fragmentation of legislation due to the margin of manoeuvre left to national legislators to maintain or introduce more specific provisions to adapt the application of certain rules. While the Council considers that this margin of manoeuvre is still justified, it believes that its development should be closely monitored’ (our own translation).

²⁷⁸ C-399/11, *Stefano Melloni v Ministerio Fiscal*, paras. 55-62.

²⁷⁹ C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd, and Maximillian Schrems*, para. 98:

‘[...] it should be noted that, although, as Article 6(3) TEU confirms, the fundamental rights enshrined in the ECHR constitute general principles of EU law and although Article 52(3) of the Charter provides that the rights contained in the Charter which correspond to rights guaranteed by the ECHR are to have the same meaning and scope as those laid down by that convention, the latter does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into EU law’.

The same interpretation was undertaken in C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen, and Secretary of State for the Home Department v Tom Watson, Peter Brice, and Geoffrey Lewis*, para. 126 ff.

²⁸⁰ C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd, and Maximillian Schrems*, paras. 101 and 102.

²⁸¹ Christopher Kuner, 2020, “Article 44: General Principles for transfer”, *op. cit.*, p. 761.

although premising that the nature of the EU competence, whether exclusive or shared, to act externally is not fully clear, highlights that ‘[...] Member States might wish to use this remaining competence for the exchange of law enforcement information with third countries, or otherwise for purposes of administrative cooperation with third countries requiring the exchange and use of personal data’²⁸². The author then comes to the conclusion that ‘[...] the existence of an exclusive EU competence under Article 16 TFEU must be assumed on the basis of the reasoning that effective protection of the fundamental rights of privacy and data protection on the internet cannot be achieved by internal rules alone. Effective protection requires the widest possible geographical scope of protection, and hence external action’²⁸³. We recall that the principle of effectiveness, or *effet utile*, of the internal regulation may justify the exclusive nature of the EU external competence for which Member States not only would have lost their treaty-making power, but also would be unable to include provisions on data protection in any agreement. In other words, the protective purpose of Article 16 TFEU might be found to be ensured by the EU better than by the Member States’ action, which triggers the *AETR/ERTA* effect. Recital (102) may support the existence of an EU exclusive implied external competence based on Article 16(1) TFEU when it finds that:

‘[...] Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects’²⁸⁴.

The possibility to constrain Member States’ treaty-making powers through secondary legislation has been experimented with in other fields too²⁸⁵, and this sentence clearly echoes the *AETR/ERTA* doctrine that requires an assessment of the principle of affectation on the basis of the concrete provisions enshrined in the GDPR and in the envisaged agreement to be concluded with third parties. However, recital (102) suggests ascertaining, on a case-by-case basis, whether internal provisions had, or had not, triggered a pre-emptive exclusivity and, consequently, whether the exercise of the EU external (implied) competence displaces the Member States’ competences. As Prof. Cremona notes, we shall distinguish between the “area” in which actions is taken, and the “elements” of that action’²⁸⁶.

²⁸² Hielke Hijmans, 2016, *op. cit.*, pp. 449-510, p. 469.

²⁸³ *Ibidem*.

²⁸⁴ Recital (102) GDPR.

²⁸⁵ Jan Klabbers, “Restraints on the treaty-making powers of Member States deriving from EU Law? Towards a framework for analysis”, in Enzo Cannizzaro, *The European Union as an Actor in International Relations*, The Hague, Kluwer Law International, 2002, pp. 151-176, pp. 165-166.

²⁸⁶ Marise Cremona, 2010, *op. cit.*, p. 104.

Notably, during the negotiations on the GDPR, the European Commission asked that the Council authorises it to negotiate the relevant Second Additional Protocol to Convention 108, as the EU is expected to finally take part in it²⁸⁷. Therefore, the Second Additional Protocol was a crucial opportunity to clarify the extent to which the EU could have acted externally. Negotiations were theoretically led by the Member States and the European Commission²⁸⁸ under the mixed formula²⁸⁹, leaving the grey areas on the internal allocation of competences²⁹⁰ as well as on their ranges²⁹¹ unclear. From the very beginning it was understandable that at least some areas – such as defence and national security – had remained jealously held within the Member States’ own sovereign prerogatives²⁹². Although the European Commission proposed to specify in its mandate that the provisions of the amended Convention 108 may have affected common rules or altered their scope within the meaning of Article 3(2) TFEU²⁹³, Member States

²⁸⁷ Council of the UE, *Comments on the recommendation for a Council decision authorising the opening of negotiations on the modernisation of Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (EST 108) and the conditions and modalities of accession of the European Union to the modernised Convention*, 6655/13 EXT 1 (18.03.2013), Brussels, 20 February 2013, and Council of the EU, *Recommendation for a COUNCIL DECISION authorising the opening of negotiations on the modernisation of Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (EST 108) and the conditions and modalities of accession of the European Union to the modernised Convention*, 16466/12 EXT 1, Brussels, 6 February 2014.

²⁸⁸ See the Council of the EU: *Negotiations on the modernisation of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of personal data (EST 108) - Information with a view to the CAHDATA - meeting on 12-14 November 2013 (Strasbourg)*, 15850/13 DCL 1, Brussels, 16 November 2018; *Negotiations on the modernisation of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of personal data (EST 108) - Preparation of the CAHDATA meeting on 1-3 December 2014 (Strasbourg)*, 13963/14 DCL 1, Brussels, 30 October 2019, and - *Follow-up to the CAHDATA meeting in Strasbourg 1-3 December 2014*, 5950/15 DCL 1, Brussels, 8 January 2019.

²⁸⁹ Council of the EU, *Draft Council Decision authorising the European Commission to participate on behalf of the European Union in the negotiations on the modernisation of Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (EST 108) and the conditions and modalities of accession of the European Union to the modernised Convention*, 7234/3/13 REV 3 EXT 1, Brussels, 25 November 2013.

²⁹⁰ See the Decision of the Committee of Ministers of the session No. 128 on *Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Elsinore, 18 May 2018, p. 32, para. 160: ‘Upon accession, the EU shall make a statement clarifying the distribution of competences between the EU and its member States as regards the protection of personal data under the Convention. Subsequently, the EU will inform the Secretary General of any substantial modification in the distribution of competences’.

²⁹¹ As Jörg Polakiewicz, *op. cit.*, p. 4, points out, in the light of the revision of the Convention 108 it was advanced the possibility for the EU to make proposals and to vote within the Committee of Ministers: ‘Notwithstanding the existence of broad EU competences in this field, the Committee of Ministers did not grant voting rights to the EU in the ad hoc committee tasked with the elaboration of the protocol (CAHDATA). This did not, however, prevent the Commission representative from speaking and negotiating on behalf of the EU Member States in practice’. As this decision has never been adopted, the European Commission must have been specifically authorised to observe the negotiations, without being entailed to negotiate within the Committee of Ministries.

²⁹² Council of the EU, 7234/3/13 REV 3 EXT 1, Brussels, 25 November 2013, p. 2.

²⁹³ Council of the EU, *Proposal for a COUNCIL DECISION authorising Member States to ratify, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)*, 9766/18, Brussels, 6 June 2018, p. 5:

refused recognise an exclusive competence as the negotiations of the data protection package were still open. On the contrary, Member States welcomed mixed negotiations and noted that Article 3(2) TFEU could not confer the EU exclusive competence unless common rules might have been affected: ‘In such circumstances, the choice of proceeding in the format of a mixed agreement is not only in accordance with EU law (including the requirements of the principle of subsidiarity) but also functionally warranted’²⁹⁴. In practice, the expertise reached at the supranational level in the data protection field made the EU’s representative the real leader in the Convention 108+ negotiations. According to Prof. Gascón Marcén:

‘The Council of Europe is a leader in this area with the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), the principles of which the European Community transposed in the 1995 Data Protection Directive. The modernisation procedure of the Convention and the Directive went in parallel resulting in the Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (known as 108+) and the General Data Protection Regulation (GDPR) respectively. However, the negotiations that were taking place within the EU were reflected in the content of the Convention's principles and provisions; in fact, the Protocol has been defined as a ‘light’ GDPR’²⁹⁵.

‘The provisions of the amended Convention No 108, to the extent they apply to processing of personal data in the context of activities falling within the scope of the Union law, may affect common rules or alter their scope within the meaning of Article 3(2) TFEU, as these provisions coincide with the obligations contained in Regulation (EU) 2016/679 of the European Parliament and of the Council and Directive (EU) 2016/680 of the European Parliament and of the Council’.

Notably, the European Commission Proposal for a Council Decision authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, COM(2021) 719 final, Brussels, 25.11.2021, supports the existence of the EU exclusive external (implied) competence based on Articles 82(1) and 16 TFEU regulating the judicial cooperation in criminal matters and the protection of personal data. However, also in this case Member States have opted for the mixed formula and they have been invited to sign it from the 12 May 2022 onward ‘chacun en leur propre nom’ – see “Le Conseil donne son feu vert pour la signature du second protocole de la convention de Budapest sur la cybercriminalité”, *Bulletin Quotidien Europe*, No. 12926, 6.4.2022. As Teresa Fajardo del Castillo, *La Diplomacia del Clima de la Unión Europea: La Acción Exterior sobre Cambio Climático y el Pacto Verde Mundial*, Madrid, Reus, 2021, p. 61, brilliantly explains (our own translation):

‘After a difficult start following the entry into force of the Lisbon Treaty, in which the European Commission would try to force its sole representation in international bodies, the pragmatism of diplomatic betrayal has meant that, at least as far as climate diplomacy is concerned, the Commission and the Member States have agreed on a truce. [...] The shared or mixed competence that has determined that international environmental agreements are all mixed agreements has also had a translation into institutional representation where the presence of the Presidency of the Union representing the Member States has been retained alongside the Commission representatives on many occasions’.

²⁹⁴ Council of the EU, *Recommendation for a Council Decision authorising the opening of negotiations on the modernisation of Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (EST 108) and the conditions and modalities of accession of the European Union to the modernised Convention*, 6176/13 DCL 1, Brussels, 30 January 2019, p. 4.

²⁹⁵ See Ana Gascón Marcén, “La Unión Europea y los convenios internacionales elaborados en el marco del Consejo de Europa”, en Paula García Andrade, *Interacciones entre el Derecho de la Unión Europea y el Derecho internacional público*, Valencia, Tirant lo Blanch, forthcoming. The author also highlights that the EU was responsible of the prolongation of the negotiations of the latest Protocol that it finally promoted in the light of the Convention 108 prominent role in the proceeding for the adoption of an adequacy decision – see *infra*.

In any case, as the EU could not adopt Convention 108²⁹⁶, it could not adopt the new Protocol either, as a result, Member States were empowered to do so on its behalf²⁹⁷. All in all, the new Protocol covers both the competences of the EU and those of its Member States²⁹⁸ but the mixed formula hides the real extent of the EU and the Member States' respective participation²⁹⁹.

²⁹⁶ Convention 108 was initially restricted to only states that were party to the Council of Europe, while the European Commission was granted observer status within the Committee of Ministers during the negotiations according to Article 23(1) of Convention 108. See also Greenleaf, Graham, "Data Protection Convention 108 Accession Eligibility: 80 Parties Now Possible (August 31, 2017)", *Privacy Laws & Business International Report*, No. 148, 2018, pp. 12-16. According to the Article 29 DPWP, *Second Annual Report*, Brussels, 30.11.1998:

'The Community, represented by the Commission, is now able to intervene within both the CJ-PD and the Consultative Committee when the items under discussion fall within the external competences resulting from Directives 95/46/EC and 97/66/EC. This was the case for the texts referred to above which have recently been adopted or are in preparation. This cooperation with the Council of Europe aims to ensure full compatibility with Community directives'

In Article 29 DPWP, *Third Annual Report*, Brussels, 22.12.2000, pp. 54-55, it was highlighted that the participation of the Community in the preparatory works of the Council of Europe's committees was aimed at ensuring its compatibility with the DPD. Provided that the Community could have not adopted the 1999 amending Protocol itself, but given that the European Community had "occupied the territory" with the adoption of the DPD, it authorised its Member States to approve the decision of the Committee of Ministers on its behalf – see the Council of the EU, *Adoption of Council Decision authorising the Member States to unanimously approve, on behalf of the European Communities, the adoption by the Committee of Ministers of the Council of Europe of amendments to allow the European Communities to accede to the Convention for the protection of individuals with regard to automatic processing of personal data (Council of Europe Convention 108)*, 8133/99, Brussels, 20 May 1999. The doctrine of delegation implies that '[...] an international agreement will be received into the EU legal order when, 'in ratifying or acceding to that agreement, the Member States acted in the interest and on behalf of' the Union and when there is EU legislation in place which functions as an incorporating device for the agreement', by Jan Willem Van Rossem, "The EU at Crossroad: A Constitutional Inquiry into the Way International Law Is Received within the EU Legal Order", in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *International Law as Law of the European Union*, Leiden, Martinus Nijhoff Publishers, 2012, pp. 59-92, p. 78. See also C-439/01, *Libor Cipra, Vlastimil Kvasnicka and Bezirkshauptmannschaft Mistelbach*, 16 January 2003, EU:C:2003:31, quoted by the own author as a paradigmatic example of the doctrine of delegation.

²⁹⁷ See the Council of the EU, *Proposal for a COUNCIL DECISION authorising Member States to sign, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No.108) - Outcome of the DAPIX meeting on 15 June 2018*, 10225/18, Brussels, 18 June 2018, and the adopted Council Decision (EU) 2019/682 of 9 April 2019 authorising Member States to ratify, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ST/10923/2018/INIT, OJ L 115, 2.5.2019, pp. 7-8. The amending Protocol authorises the EU – together with other international organisations – to become a party of the Convention 108+ and, consequently, this is granted the right to vote in the Convention Committee as stated in the Council of the EU, 9766/18, Brussels, 6 June 2018, p. 2. The Treaty Office of the Council of Europe, *Practical Guide to procedures applicable to the daily management of acts concerning the conventions of the Council of Europe*, Strasbourg, 2020, available at www.rm.coe.int, p. 44, highlights that the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data introduces a simplified procedure for which it will '[...] enter into force after acceptance or ratification by a significant number of parties and following the expiry of a period of five years. After its entry into force, the protocol would be binding only to parties which have ratified it'.

²⁹⁸ Recital (3a) of the Council of the EU, 10225/18, Brussels, 18 June 2018.

²⁹⁹ See for example the United Kingdom's position, reserving itself 'to revisit questions on competence' in Council of the EU, *Negotiations on the modernisation of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of personal data (EST 108) - Preparation of the CAHDATA meeting on 1-3 December 2014 (Strasbourg)*, 14780/14 DCL 1, Brussels, 31 October 2019, p. 39:

'[...] In particular, we are no further forward in reaching a common understanding of where the exclusive competence of the Commission begins and ends, and therefore, where Member States retain competence to negotiate in proceedings on the Convention on their own behalf. The Commission has previously indicated that they are unable to meet this demand, i.e. articulating a clear delineation between the Commission and Member

Indeed, such a mixed agreement impedes to clarify the areas in which the EU has achieved an exclusive competence³⁰⁰ and where the competence is shared with its Member States³⁰¹. Thus, the Committee of Ministers specified that: ‘Upon accession, the EU shall make a statement clarifying the distribution of competences between the EU and its member States as regards the protection of personal data under the Convention. Subsequently, the EU will inform the Secretary General of any substantial modification in the distribution of competences’³⁰². According to Polakiewicz, such a declaration:

‘[...] would not have to indicate exhaustively the list of EU competences, which are in any case evolutive in nature. Where necessary, questions related to the exact distribution of competences between the EU and its Member States could be addressed in the context of the monitoring mechanism in which both the EU and its Member States would anyway have to cooperate on the basis of the duty of loyal cooperation’³⁰³.

Yet, the presence of elements retained within the Member States’ sovereignty in relation to an underlying shared competence suggests that neither the EU nor the Member States can act on their own externally and, consequently, that the EU external exercise *vis-à-vis* the Convention 108+ can only be mixed.

Depicting the EU external competence on personal data as a non-exclusive and, specifically, a shared competence that becomes mixed in its external exercise, suits the retention by Member States of their sovereign prerogative in “protecting” human rights within their domestic constitutional systems – what Ramses A. Wessel describes as implied mixity³⁰⁴ – which is

State competence. Under these circumstances therefore we reserve the right to intervene and assert competence in these and future negotiations’.

³⁰⁰ To be noted that, in those areas where the EU is entitled of an exclusive competence it can be inferred that it is already bound by Convention 108 despite its impossibility to accede to it. Indeed, the World Trade Organisation (WTO) jurisprudence implies that the Member States have transferred their power to the EU and that the latter has succeeded to them in the international commitment previously assumed – see *infra*. Conversely, where the competence is shared, then, the situation will remain as such; specifically, although the EU may potentially accede to Convention 108, external factors prevent them from doing it for now.

³⁰¹ See the French position claiming to clarify what should be intended for EU *acquis* in the Council of the EU, 14780/14 DCL 1, Brussels, 31 October 2019, p. 18. In favour of a shared competence seems to be Santa Slokenberga, *loc. cit.*

³⁰² See the Decision of the Committee of Ministers of the session No. 128 on *Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Elsinore, 18 May 2018, para. 160.

³⁰³ Jörg Polakiewicz, “A Council of Europe perspective on the European Union: Crucial and complex cooperation”, *Europe and the World: A law review*, Vol. 5, No. 1, 2021, pp. 1-19. Similarly, Prof. Gascón Marcén, *loc. cit.*, affirms: ‘However, this is something of a “snapshot” because in reality the EU tends to exercise competences in more areas over time, which can lead to some uncertainty for non-EU states parties to a convention who are not themselves EU parties and who may not necessarily be fully familiar with the EU’s dynamic assumption of new competences’ (our own translation).

³⁰⁴ Ramses A Wessel, 2012, *op. cit.*, pp. 43-44, highlights that with the EU PNR Agreements, although directed to the EU – i.e., air carriers to be scrupulous –, ‘the content of the obligation potentially affects fundamental rights – especially the right to the protection of personal data –, that are usually protected by national constitutions through the right to privacy’. “Horizontal mixity”, instead, refers to cross-cutting agreements covering domains belonging to Maastricht’s various pillars, in which case European Community’s policies must have preference over EU ones

reflected in the Member States' choice in heading Article 16(1) TFEU with the same words used in Article 8 CFREU, while relegating this task to the international legal order only subsidiarily³⁰⁵. This approach supports our findings in Chapter I where we concluded that the supra-national level subsidiarily complements the national one as the EU may intervene to safeguard the individual's human rights only after the domestic courts have ruled. Although through the GDPR the EU may have reached exclusive competence in certain elements – e.g., the adoption of adequacy decisions – and, consequently, the ability to make the relevant assessment, Member States are not restrained from transferring personal data toward third parties. Indeed, appropriate safeguards and derogation clauses enable them to maintain a certain flow of data, though with weaker guarantees from a human rights perspective. In addition, in the frame of adequacy decisions where the EU may be deemed to be exclusively competent, the need to evaluate a third party's 'public security, defence, national security and criminal legislation'³⁰⁶ calls for the Member States participation in the external sphere. Therefore, the co-presence of elements of shared competence with the insertion of a national security clause, suggests that the EU external (implied) competence stemming from Article 16 TFEU can be concretised in mixed agreements where the EU shares the external action with its Member States. If this is the case, preferring the adoption of an adequacy decision over the conclusion of an international (mixed) agreement saves the European Commission and the Member States the long and tortuous process – first experimented with in Convention 108+ – that culminates with the unanimity vote in the EU Council³⁰⁷.

2.2.2. The Law Enforcement Directive

As a Directive, the LED is firstly directed to the Member States that are responsible for balancing the respect of fundamental rights and freedoms with the need to exchange personal

– see C-91/05, *Commission of the European Communities v Council of the European Union*. Finally, “vertical mixed” agreements were used to regulate the pre-Lisbon EU/Member States relationship, as Ramses A. Wessel, p. 43, notes: The ‘[...] fulfilment of the obligation by the EU entails the obligation for Member States to apply the extradition system established by the agreement’.

³⁰⁵ See *infra* our analysis on the enforceability of ‘legally binding instruments’.

³⁰⁶ Article 45(2)(a) GDPR and Marc Maresceau, 2010, *op. cit.*, p. 16.

³⁰⁷ Precisely because of the presence of the EU and its Member States, they are more difficult to negotiate and need the ratification of all national Parliaments – see Jörg Monar, *op. cit.*, p. 24, and David O’ Keeffe and Henry G Schermers, *Mixed Agreements*, Deventer, Kluwer, 1983, pp. 9 and 10. Christiaan Timmermans, “Opening Remarks – Evolution of Mixity Since the Leiden 1982 Conference”, in Christophe Hillion and Panos Koutrakos, *op. cit.*, pp. 1-8, points out how these problems develop on different layers: institutionally, during the negotiations and the conclusion of the agreement; internally, when delimiting the nature of the competences conferred to the EU; *ex post*, with regard to their interpretation and the control of compatibility by the CJEU; and, finally, when allocating the responsibility in case of non-compliance with the obligations undertaken.

data³⁰⁸. The LED does not, as desired, explicitly state the level of harmonisation it seeks to achieve within its dispositions. As with the DPD, the LED calls for the EU legislator to suppress existing obstacles deriving from the Member States' divergent legislations on the protection of personal data³⁰⁹ while ensuring '[...] a high level of protection within the Union'³¹⁰. Even more relevant is the explicit provision legitimising the Member States to adopt more stringent rules to guarantee a higher level of protection to individuals' fundamental rights on personal data³¹¹. These considerations suggest that the LED aims to lay down minimal standards of protection while leaving a huge margin of manoeuvre to the Member States to adopt higher standards³¹². On this basis, the EU can conclude international agreements without triggering the *AETR/ERTA* exclusivity on the Member States' treaty making power, provided that the agreement to be concluded respects the same degree of approximation. Specifically:

'[...] when the Union adopts less stringent rules than those in a convention, then Member States can adopt more stringent measures than those provided in EU secondary law, by applying the (stricter measures of) the international agreement. Secondly, if the Union passes more stringent measures than those of the (minimum standard setting) international agreement, that agreement does not prevent the full application of the more stringent Union measures by the Member States. It could be added that in the second case, neither the agreement nor the Union measures would bar Member States to regulate even stricter measures than foreseen by both acts. Thus, the ERTA pre-emption principle does not apply if both the international agreement and the provisions of Union law provide minimum standards'³¹³.

³⁰⁸ Article 1(2) LED.

³⁰⁹ Recital (15), first sentence, LED: 'In order to ensure the same level of protection for natural persons through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between competent authorities'.

³¹⁰ Recital (15) LED, second instance.

³¹¹ Recital (15) LED, last sentence: 'Member States should not be precluded from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities'. See also Article 1(3) LED: 'This Directive shall not preclude Member States from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities'.

³¹² See the German position in the Council of the EU, 6846/14 ADD 3, Brussels, 28 March 2014, p. 5: 'There should be fundamental agreement that the Directive sets only minimum standards'.

³¹³ Marcus Klamert, "What We Talk About When We Talk About Harmonisation", *Cambridge Yearbook of European Legal Studies*, No. 17, 2015, pp. 360-379, p. 377. The author maintains that 'minimum harmonisation' enables Member States to adopt further requirements that are not strictly necessary under the EU legislation. Klamert affirms that 'minimum harmonisation' is more cooperative than 'full harmonisation' as it is in the case of directives that impose to the Member States' to cooperate to co-opt to achieve a pre-determined objective. It is also relevant his distinction between 'legislative minimum harmonisation' and 'constitutional minimum harmonisation' to define the Member States' prerogative in adopting more stringent rules for a legislative choice or on the basis of the Treaty's provisions as he observes that only in the former the CJEU maintains that national measures shall respect the principle of necessity and proportionality with respect to the objective pursuit.

The EU-US Umbrella Agreement concluded in 2016 is a good example of this practice³¹⁴. The EU-US Umbrella Agreement was concluded on the basis of Article 16 TFEU, which allowed the EU to avoid the uncomfortable interpretation of the Declaration No 36 on Article 218 of the TFEU concerning the negotiation and conclusion of international agreements by Member States relating to the AFSJ annexed to the Lisbon Treaty. According to this Declaration:

‘The Conference confirms that Member States may negotiate and conclude agreements with third countries or international organizations in the areas covered by Chapters 3, 4 and 5 of Title V of Part Three in so far as such agreements comply with Union law’.

The wording suggests that EU external action in these areas shall always be considered as shared, yet the correct manner in which to interpret such a Declaration is not clear among the scholars. Prof. García Andrade highlights that in *Opinion I/03* the CJEU had already declared that the EU external action in civil judicial matter was exclusive by nature³¹⁵, so the Declaration cannot override the *AETR/ERTA* doctrine. In her opinion, Declaration No 36 imposes on the Member States the duty to comply with EU law where the praetorian doctrine has been already integrated³¹⁶. However, Prof. Matera affirms that the Declaration No 36 should be interpreted so as to exclude the pre-emptive effect of EU international agreements. He also explains that given that the provisions under Chapters 4 and 5 of Title V TFEU are mainly concerned with approximation, with a clear predominance of minimum standards, ‘[...] it is possible to conclude that, *de iure condito*, conflicts, in relation to the exclusive nature of the external competence, should not emerge’³¹⁷. Furthermore, such a Declaration can be confronted with the previous Article 133(5) of the 2002 TEC, which enabled Member States ‘to maintain and conclude agreements with third countries or international organisations in so far as such agreements comply with Community law and other relevant international agreements’ that has also received contrasting interpretations. Some scholars have stated that this clause preserves Member States’ action notwithstanding the European Community’s intervention, whether

³¹⁴ The negotiations dates back several years ago: see the EDPS, *Contribution of the EDPS to the consultation on the future EU-US international agreement on personal data protection and information sharing for law enforcement purposes*, Brussels, 12.03.2010. On the EU-US relationship on the transfer of personal data, including the Umbrella Agreement, Cristina Blasi Casagran, 2017, *op. cit.*, pp. 100-111, states that the US has a different cultural background for which the right to the protection of personal data is not safeguard *per se* but it is associated to the right to a private life. For this reason, principles such as data minimisation, storage limitation, and the publication of criminal records are highly different treated in the US with respect to the EU.

³¹⁵ Paula García Andrade, 2015, *op. cit.*, p. 219.

³¹⁶ In the same line see Ramses A. Wessel, Luisa Marin, and Claudio Matera, “The External Dimension of the EU’s Area of Freedom, Security and Justice”, in Christina Eckes and Theodore Konstadinides, *Crime within the Area of Freedom, Security and Justice: A European Public Order*, Cambridge, Cambridge University Press, 2011, pp. 272-300, p. 297.

³¹⁷ Claudio Matera, 2016, *op. cit.*, pp. 145 and 146.

internal or external³¹⁸; others, instead, maintain that Member States cannot escape the *AETR/ERTA* doctrine³¹⁹. Specifically, Prof. De Baere found that the *AETR/ERTA* doctrine:

‘[...] cannot be deduced from the requirement that agreements concluded by the Member States should comply with Community law. [T]he ERTA doctrine applies regardless of whether the agreement in question complies with the Community law. The implication of Member States retaining their external competence as long as the international agreements concluded by them comply with Community law thus must be that the ERTA doctrine as traditionally understood does not apply’³²⁰.

This interpretation confirms that the EU external competence may be exclusive or shared with the Member States depending on whether the *AETR/ERTA* affectation doctrine applies or not. Although it is true that EU criminal law still limits the EU action by limiting its mandate to the adoption of minimum standards, or by directly excluding harmonisation in several dispositions, this is not the case of Article 16(2) TFEU, as it does not lower the level of the EU intervention. As a result, by opting to use this legal basis alone, the EU can avoid such uncertainty. All in all, the suppression of the pillars structure and the crosscutting position of Article 16 TFEU enables the EU to rely on this legal basis to regulate the protection and flow of personal data for law enforcement purposes too³²¹. Yet, as the EDPS noted, some discrepancies between the EU-US Umbrella Agreement and the LED are visible: first, the EU-US Umbrella Agreement has a limited scope *rationae personae* as it excludes the nationals of third countries while giving priority to EU and US citizens³²²; second, the definition of “processing” does not include some type of operations, such as recording, storage, retrieval, consultation, alignment or combination, blocking, erasure or destruction. Finally, the EDPS noted that the right to access and to rectify personal data has been unduly restricted by virtue of broader clauses, such as one granting law enforcement access to sensitive information or the recommendation to reduce existing derogations.

As we advanced above, the EU-US Umbrella Agreement seeks ‘[...] a high level of protection of personal information and enhance cooperation between the United States and the European Union and its Member States, in relation to the prevention, investigation, detection or prosecution of criminal offences, including terrorism’³²³ for which purpose it establishes

³¹⁸ Marise Cremona “The External Dimension of the Single Market: Building (on) the Foundations”, in Catharine Barnard and Joanne Scott, *The Law of the Single European Market: Unpacking the Premises*, London, Hart Publishing, 2002, pp. 351-394, p. 379.

³¹⁹ Horst Günter Krenzle and Christian Pitschas, “Progress or Stagnation? The Common Commercial Policy After Nice”, *European Finance Review*, No. 6, 2001, pp. 308-309.

³²⁰ Geert De Baere, 2008, *op. cit.*, p. 64.

³²¹ See Chapter I.

³²² Which is a clear consequence of the US legislation on data as explained by Hielke Hijmans, 2016, *loc. cit.*

³²³ Article 1(1) of the EU-US Umbrella Agreement. This excludes the possibility that the Umbrella Agreement is a soft law measure.

“standards of protection” on the transfer of personal data between competent authorities established in the US and the EU respectively, without it constituting a valid legal basis for the enabling of the transfer of personal information³²⁴. This option had been suggested by the EDPS when it underlined that ‘[...] common minimum standards as recognised in a binding instrument could facilitate any further discussion on the transfer of personal data in relation to a specific database or processing operations’³²⁵. In this sense, the establishment of a *de minimis* legislation does not differentiate from framework agreements. As Prof. Fajardo del Castillo maintains: ‘[...] each framework agreement triggers an ongoing negotiating process that informs its future regulatory development and its own institutional structure’³²⁶. The dispositions set forth in the EU-US Umbrella Agreement are called to supplement the provisions on the protection of personal data inserted in other EU-US treaties, and other agreements concluded between the Member State/s and the US³²⁷. Its programmatic nature generates the expectation that further protocols or new treaties will be concluded on its basis³²⁸. For example, the EU-US Umbrella Agreement is invoked by the EU-US e-Evidence Agreement where private service providers will have to disclose the data they owe to foreign law enforcement authorities³²⁹.

If it is clear that the EU-US Umbrella Agreement is exercise of the EU external (implied) competence based on the LED, it is more difficult to assess whether this Agreement constitutes a valid legal basis to transfer personal data. According to the EDPS, the EU-US Umbrella Agreement introduces a ‘presumption of compliance’ that should have been accompanied by the US commitment to transpose the data protection principles into the US legal order³³⁰. Alongside this, the EDPS queried if the transfer of data falling within the scope of the Agreement should have been considered to comply with data protection principles, without the

³²⁴ Article 1(3) of the EU-US Umbrella Agreement.

³²⁵ Opinion of the EDPS on *the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection*, (2009/C 128/01), Brussels, 6.6.2009, para. 35.

³²⁶ Teresa Fajardo del Castillo, 2018, *op. cit.*, pp. 23-51, p. 35 (our own translation).

³²⁷ Article 5(1) of the EU-US Umbrella Agreement.

³²⁸ Opinion of the EDPS on *the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection*, Brussels, 6.06.2009, para. 32:

‘The EDPS supports the preference in the report for a binding agreement. An official binding agreement is in the view of the EDPS an indispensable prerequisite to any data transfer outside the EU, irrespective of the purpose for which the data are being transferred. No transfer of data to a third country can take place without adequate conditions and safeguards included in a specific (and binding) legal framework. In other words, a Memorandum of Understanding or another non-binding instrument can be useful to give guidance for negotiations for further binding agreements, but can never replace the need for a binding agreement’.

³²⁹ See *infra* in this Chapter.

³³⁰ Preliminary Opinion of the EDPS No. 1/2016 on *the agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences*, Brussels, 12.02.2016, p. 8.

need of any further authorisation. Although the EDPS initially suggested giving direct effect to the EU-US Umbrella Agreement's dispositions in order to be invoked before CJEU and, consequently, to ensure the effectiveness of the measures adopted in the national legal orders for its transposition³³¹, the *de contrahendo* nature of the Agreement suggests that it has to be transposed and concretised in forthcoming agreements and protocols³³². Consequently, the EDPS confirmed that in no way can the EU-US Umbrella Agreement replace the adoption of an adequacy decision³³³ or, we should add, appropriate safeguards³³⁴. The EDPS stated that the US should agree to a minimum level of protection on a case-by-case basis. Such an assessment would include the existence of reciprocity agreements in the following areas: substantive provisions on data protection; redress mechanisms and, finally, access by law enforcement authorities to personal data. Specifically, the EU-US Umbrella Agreement should have prohibited pull systems of data extraction under the supervision of data protection authorities or the judicial authorities, in compliance with applicable and reciprocal substantive and procedural dispositions³³⁵. In other words, the transfer of data to the US should have been backed up by a data request model that, according to the principle of proportionality, is made on an *ad hoc* basis. Indeed, the EDPS confirmed that: 'Permanent access by third country law enforcement authorities to databases situated in the EU would be considered as disproportionate and insufficiently justified'³³⁶. At present, the EU-US Umbrella Agreement provides for numerous soft law clauses – see for example the ones on 'as appropriate'³³⁷, 'where

³³¹ Opinion of the EDPS on *the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection*, Brussels, 6.06.2009, para. 34.

³³² This does not prevent the Agreement from deploying any effect in the domestic legal orders. As Luigi Condorelli, "Il Giudice italiano e i trattati internazionali: Gli accordi self-executing e non self-executing nell'ottica della giurisprudenza", *Rivista di diritto internazionale privato e processuale: Studi e pubblicazioni*, No. 12, Padova, CEDAM, 1974, p. 69, highlights: '[...] even covenanted programmatic norms may have to be considered operative, and therefore self-executing, whenever the domestic legal system is already in such a "state" as to transpose their indications' (our own translation).

³³³ Opinion of the EDPS on *the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection*, Brussels, 6.06.2009, para. 41:

'The EDPS considers that only a real adequacy test would ensure sufficient guarantees as to the level of protection of personal data. He considers that a general framework agreement with a scope as broad as the one of the HLCG report would have difficulties to pass, as such, a real adequacy test. The adequacy of the general agreement could be acknowledged only if it is combined with an adequacy of specific agreements concluded on a case by case basis'.

³³⁴ Another reading suggests to interpret Article 37(1)(a) LED for which the transfer of personal data may occur on the basis of 'a legally binding instrument' as excluding the requisite of enforceability as Article 46(2)(a) GDPR clearly states – i.e., 'a legally binding and enforceable instrument'. This interpretation would lead us to conclude that actually the EU-US Umbrella Agreement is a valid legal basis to transfer personal data. Waiting for a CJEU ruling, we decided to opt for the first, more guaranteeing, interpretation as we have already advanced above.

³³⁵ Opinion of the EDPS on *the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection*, Brussels, 6.06.2009, paras. 45-49.

³³⁶ *Ibid.*, para. 62.

³³⁷ Article 5(1), 17(1) last paragraph, and 21(1)(c) of the EU-US Umbrella Agreement.

appropriate³³⁸, ‘to the extent relevant’³³⁹ – that substantially weaken its binding force³⁴⁰. That being said, the Agreement is viewed as a model to be followed by the EU in the creation of new international agreements with third parties in fields covered by the LED³⁴¹. However, the Article 29 DPWP pointed out two major shortcomings that deserve further attention³⁴²: first, the EU-US Umbrella Agreement does not cover cases of national security that are kept under the sovereign competences of the Member States³⁴³ and, second, the Agreement does not regulate the access of third countries’ authorities to data processed by private companies.

With regard to the first point, the Article 29 DPWP specified that the national security clause set forth in Article 4(2) TEU defines the competence of the EU only *vis-à-vis* its Member States and cannot be used by data protection controllers operating under EU law to comply with a third country’s request for the transfer or disclosure of personal data according to their concept of “national security”³⁴⁴. In its words:

‘Since the Umbrella Agreement will fall short in offering full protection to all citizens, what is needed is an international agreement providing adequate protection against indiscriminate surveillance [...] However, this agreement would be directly linked to the national security exemption and thus fall outside the scope of EU law. Therefore, it is up to the Member States to start negotiations in a coordinated manner’³⁴⁵.

Given that national security is kept within the prerogatives of the Member States, the latter are the only ones entitled to conclude an international agreement regulating the transfer or access to personal data by surveillance agencies. Nevertheless, some grey areas still exist,

³³⁸ Article 14(3) *in fine*, 18(3), and 21(1)(a) of the EU-US Umbrella Agreement.

³³⁹ Article 23(3) and 24(2) of the EU-US Umbrella Agreement.

³⁴⁰ Article 1 of the EU-US Umbrella Agreement. On soft law see: Teresa Fajardo del Castillo, 2018, *op. cit.*, and César Nava Escudero, “El acuerdo de París. Predominio del soft law en el régimen climático”, *Boletín Mexicano de Derecho Comparado*, No. 147, Vol. 49, 2016, pp. 99-135: ‘First, the very flexibility or elasticity of the soft law rule allows States to reach a certain consensus on an environmental issue, which would not be achieved if the very nature of the precept were too stringent [...] Second, the soft law rule is a very useful tool that assumes (though not infallibly) a win-win scenario for all States and the treaty objective in question, at least in temporal terms and with the expectation that this will be the case’ (our own translation).

³⁴¹ As it was already prospected by the Article 29 DPWP, *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, Brussels, 1.12.2009, para. 35.

³⁴² Opinion of the EDPS No. 04/2014 on “*Surveillance of electronic communications for intelligence and national security purposes*”, Brussels, 3.04.2014, p. 15.

³⁴³ Article 3(2) of the EU-US Umbrella Agreement.

³⁴⁴ Working Document of the Article 29 DPWP on *surveillance of electronic communications for intelligence and national security purposes*, Brussels, 5.12.2014, p. 25. The sole exception can be envisaged when the third country’s security interest is also shared by the Member State in which case the Article 29 DPWP recognised that ‘[...] the boundaries of an EU Member State’s national security may not always be clear’ (p. 26). Nevertheless, it also specified that the mere allegation of national security interest cannot prevent EU law to be applicable. As it is the case for national security interest, a third country’s one shall be clearly set out in national law, including, where it is sealed by an international treaty between the Member State and such a third party.

³⁴⁵ Opinion of the EDPS No. 04/2014 on “*Surveillance of electronic communications for intelligence and national security purposes*”, Brussels, 3.04.2014, pp. 15 and 16.

specifically where law enforcement authorities and intelligent services cooperate under the aegis of the national security clause³⁴⁶. These uncertainties prevent a clear demarcation between the EU and the Member States' competences in the national security field. As a result, the mixed formula is once again the ideal solution that allows leaving the burdens of conferral unresolved³⁴⁷. Indeed, national security is a useful buffer for the Member States to claim the non-attribution of competences so as to curb the EU from intervening. Therefore, its exclusion from the EU-US Umbrella Agreement may be justified by the fact that the EU sought to avoid a mixed agreement.

As for the second aspect, the Article 29 DPWP pointed out that the EU-US Umbrella Agreement does not cover the possibility that third countries' authorities are given access to private companies' data processed under EU law, which was highly recommended by the EDPS³⁴⁸. As we analysed in Chapter I, the exclusion of the private sector from the Agreement is in line with the CJEU's jurisprudence binding law enforcement authorities to the data protection principles stemming from the derogations foreseen in the GDPR instead of the rules set forth by the LED. Indeed, the LED clearly refers to the exchange of data between public authorities alone, any interrelation with private individuals goes back to the GDPR, triggering the conclusion of an ex-first/third pillars "horizontal mixed" agreement³⁴⁹. If this was the intention of the contracting parties, it would be useful to make it explicit for the sake of legal certainty, as the GDPR and the LED differ on many points.

3. The conclusion of "legally binding (enforceable) instruments"

We have pointed out that the GDPR, but not the LED, states that the transfer of personal data based on an international agreement must comply with the requirement of "enforceability"³⁵⁰. The same dichotomy is recalled by the EUDPR that refers to 'a legally binding and enforceable instrument between public authorities or bodies'³⁵¹ or to 'an international agreement [...] concluded between the Union and that third country or

³⁴⁶ Working Document of the Article 29 DPWP on *Surveillance of electronic communications for intelligence and national security purposes*, Brussels, 5.12.2014, p. 26.

³⁴⁷ Article 29 DPWP Opinion No. 04/2014 on *Surveillance of electronic communications for intelligence and national security purposes*, Brussels, 10.04.2014, p. 16: 'Due account should be given to the clear identification of which of the surveillance activities described would indeed be covered by national security, and which are rather more related to law enforcement and foreign policy purposes, areas which would fall under Union law. This would trigger the possibility for EU institutions to participate more closely in case steps are taken in this direction'.

³⁴⁸ Opinion of the EDPS on *the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection*, Brussels, 6.06.2009, paras. 19-23.

³⁴⁹ See *supra*.

³⁵⁰ Article 46(2)(a) GDPR and Article 37(1)(a) LED.

³⁵¹ Articles 48(2)(a) EUDPR.

international organisation pursuant to Article 218 TFEU adducing adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals³⁵². However, we have not clarified what the term “enforceability” means, and hence its importance, as far as international agreements are concerned. If it is clear that soft law measures are excluded from the “legally binding” definition³⁵³ in full compliance with Article 216(2) TFEU³⁵⁴, we believe that the enforceability requisite leaves several unresolved concerns as a result of its vagueness and the lack of a clear definition³⁵⁵.

Notably, the European Commission’s Proposal for a Regulation on the GDPR did not provide for “legally binding (enforceable) instrument” as a means to transfer personal data³⁵⁶. The proposed Article 41 was split into two main parts: its first paragraph regulated the adoption of appropriate safeguards, while its second paragraph laid down some of the ‘legally binding instrument[s]’ that could have been adopted – e.g., binding corporate rules³⁵⁷. During the

³⁵² Article 94(1)(b) DPPE.

³⁵³ As Daniel Bodansky, “Legally binding versus non- legally binding instruments”, *Towards a Workable and Effective Climate Regime*, pp. 155-165, p. 159, notes: enforceability is not a synonym of ‘legally binding’ so that an instrument may be enforceable and not binding, but not *vice versa*. This implies that a non-binding instrument may also be enforceable if it provides for the application of sanctions in case of non-respect.

³⁵⁴ The disposition recalls the principle of *pacta sunt servanda* set forth under Article 26 of the Vienna Convention on the Law of Treaties of 23 May 1969 while stating that: ‘Agreements concluded by the Union are binding upon the institutions of the Union and on its Member States’. Jan Willem Van Rossem, *op. cit.*, p. 66, affirms that:

‘As regards treaties to which the EU is a party, the question whether an international norm is binding upon the EU is usually answered by referring to the Council act concluding the agreement. Once it has been established that an international norm is indeed binding, this subsequently means that the norm automatically, that is without the need for additional act of transformation, becomes an integral part of the Union legal order. Formally, the Treaty mechanism by which this incorporation takes place is Article 216(2) TFEU, which provides that agreements concluded by the Union are binding upon the institutions and the Member States. As ‘binding’ here means binding as a matter of EU law, Article 216(2) TFEU thus constitutes the constitutional bridge between international legal order and the EU legal order [...]’.

A separate question is that of discerning who is bound, especially in the case of mixed agreements in which the Union and its States co-participate without it always being clear who is responsible in the light of the rules of international law.

³⁵⁵ See the position of the Hungarian and Polish delegations in the Council of the EU, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – Partial General Approach on Chapter V*, 10349/14, Brussels, 28 May 2014, p. 25, and the *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Partial General Approach on Chapter V*, 10349/14 COR 1, Brussels, 11 June 2014.

³⁵⁶ See the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 011 final, Brussels, 25.01.2012.

³⁵⁷ Council of the EU, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, 5853/12, Brussels, 27 January 2012. Article 41(5) – also labelled as the ‘MoU solution’ – established that:

‘Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set

negotiations surrounding that Article, debates arose on the need to insert an explicit reference to an ‘agreement’, as the Belgian government’s comment shows: ‘[Belgium] wants to be sure to cover, for example, the international health regulations’³⁵⁸. The Belgian delegation underlined that neither model contracts, nor binding corporate rules, applied to public authorities that, instead, should have been entitled to use cooperation agreements or unilateral undertakings. Despite its provision, the concept of a “legally binding enforceable instrument” remains unclear³⁵⁹.

3.1. Enforcement in public international law

Lacking its own organic apparatus, international law manages the issuance, ascertainment, and enforcement of international norms thanks to the attribution of these functions to the state:

‘[international law] only demands, in very general terms, that is complied with. Precisely which effects international law may have in domestic or ‘municipal’ legal systems is a matter largely left to such a system’s basic rules’³⁶⁰.

The concept of “enforceability”, then, assumes different connotations in international treaty law³⁶¹:

- first, domestic enforcement requires the transposition of a treaty into the domestic legal order;
- second, automatic enforcement infers that the treaty has direct effects on the domestic order³⁶², and

of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer’.

³⁵⁸ Specifically, Belgium proposed to insert a reference to ‘cooperation agreements or unilateral undertaking by public authorities’ finding the reference to ‘administrative arrangements providing the basis for such transfer’ not clear in the Council of the EU, 6723/13, Brussels, 26 February 2013 (04.03), pp. 7 and 8.

³⁵⁹ Confront the Slovak Republic’s position in Council of the EU, 6723/13, Brussels, 26 February 2013 (04.03), p. 58, according to which: ‘Generally we understand legally binding instrument as a legal provision/procedure according to law containing a certain level of legal power and which is binding for the same range of audiences and its enforcement is real. It must also be an instrument that will be or is already enshrined in the legal system of concerned country or international organisation’. The Guidelines of the EDPS No. 2/2020 on *articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies*, Brussels, 15.12.2020, p. 17, contemplates that at least three categories of instruments may be included within the concept of legally binding (enforceable) instruments, notwithstanding their bilateral or multilateral nature, namely: international treaties; public-law agreements, and self-executing administrative agreements.

³⁶⁰ Piet Eeckhout, *EU External Relations Law*, Oxford, Oxford University Press, 2012, p. 234.

³⁶¹ Notably, the term “enforceability” must be taken aside from those of “compliance”, “implementation”, and of “justiciability” some of which are clarified Teresa Fajardo del Castillo, 2018, *op. cit.*, p. 38; Piet Eeckhout, 2012, *op. cit.*, pp. 323-438; Eleftheria Neframi, 2012, “Mixed Agreements as a source of European Union Law”, *op. cit.*, pp. 325-352; Jan Willem Van Rossem, *op. cit.*, p. 66, and Riccardo Pisillo Mazzeschi, “Responsabilité de l’État pour violation des obligations positives relatives aux droits de l’homme”, *Collected Courses of the Hague Academy of International Law*, Vol. 333, 2008, pp. 175-506, p. 265 ff.

³⁶² Enzo Cannizzaro, “The Neo-Monism of the European Legal Order”, in Enzo Cannizzaro, Paolo Palchetti, and Ramses A Wessel, *op. cit.*, pp. 35-58, p. 38, recalls that the direct effect of a treaty’s provisions may be deuced

- third, horizontal enforcement regulates states' obligations to ensure compliance with international law.

3.1.1. Domestic enforcement

The transposition of international treaty law is regulated by the monism/dualism dialectic that aims at giving effect to a treaty, or one of its dispositions, in general terms or with regard to a particular case³⁶³. As part of these terms, the concept of enforceability ensures that a legislator work at '[...] turning paper into reality or, more eloquently, translate a set of legal standards designed to influence human and institutional behaviour into social reality'³⁶⁴.

On the EU side, international agreements are considered to 'form an integral part of the EU legislation'³⁶⁵ in the terms developed by the CJEU³⁶⁶ that '[...] tends to regard domestic implementation as a means for securing compliance with international obligations and for enhancing effectiveness'³⁶⁷ so that '[...] international law is part of European Union law without need for any special act of incorporation, and it prevails over inconsistent European legislation'³⁶⁸. According to the CJEU, international agreements are settled below EU primary law but above EU secondary law as well as national law³⁶⁹. For Prof. Wright and Prof. De Hert:

'Enforcement typically means the activity of a regulator to ensure that third parties comply with a law or regulation or code. If regulators do not enforce laws or regulations or codes or do not have the resources, political support, or wherewithal to enforce them, they effectively eviscerate and make meaningless such laws or regulations or codes, no matter how laudable or well-intentioned'³⁷⁰.

However, the transposition of international law in the EU legal order is difficult to explain in light of Article 35 of the Vienna Convention on the Law of Treaties of 23 May 1969³⁷¹. Before a "pure" monist approach³⁷², some authors maintain that pluralism rather than

from its clear, precise and consistent wording – as it is internally granted to EU Directives – or because of '[...] the international nature of the provision and the purpose assigned to it in the international legal order from which it emanates'.

³⁶³ Francesco Salerno, *Diritto internazionale: Principi e norme*, Padova, 2020, 415 ff.

³⁶⁴ David Wright and Paul De Hert, 2016, *op. cit.*, p. 2.

³⁶⁵ Article 216(2) TFEU and, for example, Piet Eeckhout, "The Integration of Public International Law in EU Law: Analytical and Normative Questions" in Piet Eeckhout and Manuel López Escudero, *The European Union's external action in times of crisis*, Oxford, Hart Publishing, 2016, pp. 189-204, pp. 189-204.

³⁶⁶ C-181/73, *Haegeman v Belgium*.

³⁶⁷ *Ibid.*, para. 37.

³⁶⁸ Enzo Cannizzaro, 2012, *op. cit.*, p. 36.

³⁶⁹ Alessandra Gianelli, *loc. cit.*

³⁷⁰ *Ibid.*, p. 4.

³⁷¹ Its Article 35 states: 'An obligation arises for a third State from a provision of a treaty if the parties to the treaty intend the provision to be the means of establishing the obligation and the third State expressly accepts that obligation in writing'.

³⁷² Robert Schütze, 2010, *op. cit.*, pp. 76-77, following the C-181/73, *Haegeman v Belgium*.

constitutionalism better explains the coexistence of states and international organisations' legal orders³⁷³. According to these authors, the 'Unionisation' of international law³⁷⁴ aims at transposing international law into the EU legal order, while preserving its autonomy. In other words, EU rules filter international rules notwithstanding the Member States' monist/dualist approach, which positions the EU legal system closer to a dualist model rather than a monist one³⁷⁵.

International commitments achieve their efficacy through the EU's principles of primacy and direct effect³⁷⁶, principles that guard the uniform interpretation and application of international law within the EU supranational order. In this regard, the CJEU plays a crucial role while uniformly interpreting the provisions of international agreements, for example, through preliminary requests³⁷⁷. As treaties form an 'integral part of EU law', their enforcement is ensured by the appropriate tools regulating the implementation of Union law in the Member States' domestic legal orders³⁷⁸ which, as a last resort, triggers the European Commission's infringement proceeding³⁷⁹.

³⁷³ See Ramses A. Wessel, "Relationship Between International and EU Law", in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *op. cit.*, pp. 7-34.

³⁷⁴ Anne Peters, "The position of International Law Within the European Community Legal Order", *German Yearbook of International Law*, No. 9, Vol. 40, 1997, pp. 34-35, and Jan Wouters, André Nollkaemper and Erika de Wet, *The Europeanisation of International Law: The Status of International Law in the EU and its Member States*, The Hague, TMC Asser Press, 2008. Is the EU also responsible for agreements concluded by one, some or all of its Member States on its behalf? Marise Cremona, 2012, *loc. cit.*, suggests that the EU may be responsible for implementing such an agreement – directly in case the EU has succeeded to its Member States in the light of the WTO jurisprudence, or indirectly through its implementation – and, although its incorporation is not made through a Council decision concluding the agreement, the EU is bound by it when it has succeeded to its Member States' commitment – i.e., it has acquired an implied external exclusive competence. If not, and where the transposition occurs through the adoption of a legislative instrument – regulation, directive, or decision –, this is not placed above but within EU secondary law. Although the regulation is not apt to review the validity of EU norms, it is considered to be a parameter for their interpretation in the light of the principle of good faith set forth in Article 31(1) Vienna Convention on the Law of Treaties of 23 May 1969.

³⁷⁵ Christina Eckes, *op. cit.*, p. 368.

³⁷⁶ See *infra*.

³⁷⁷ C-53/96, *Hermès International (a partnership limited by shares) and FHT Marketing Choice BV*, 16 June 1998, EU:C:1998:292, and C-337/95, *Parfums Christian Dior SA and Parfums Christian Dior BV and Evora BV*, 4 November 1997, EU:C:1997:517.

³⁷⁸ Yet in C-402/05 P and C-415/05 P, *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities*, the General Court had been largely criticised because of its reluctance in entering into evaluating the validity of the UN Security Council's resolution not so much toward the EU domestic legal order, but *vis-à-vis* international law standards, that is, *ius cogens* norms, customary international law and, specifically, human rights – see Paolo Palchetti, "Judicial Review of the International Validity of UN Security Council Resolutions by the European Court of Justice", in Enzo Cannizzaro, Paolo Palchetti, and Ramses A Wessel, *op. cit.*, pp. 379-394.

³⁷⁹ Article 258 TFEU.

3.1.2. Direct enforcement

In the lack of transposition of an international treaty, or in case such a transposition does not comply with the international law³⁸⁰, a treaty's dispositions can be conferred the ability to take direct effect so that the agreement can be “automatically enforced” before EU and national courts. In Prof. Maresceau's words:

‘Where international agreements were directly effective, they could be automatically enforced by the executive and judicial branches of the Union and the Member States. International agreements would not just be binding ‘on’ the Member State, but also ‘in’ the Member States’³⁸¹.

Prof. Maresceau reports that “direct effect” should be appraised by a two-step approach: first, whether the provision at stake contains ‘a clear and precise obligation which is not subject, in its implementation or effects, to the adoption of any subsequent measure’ or not – as it is internally granted to EU directives³⁸² – should be evaluated; second, the wording, purpose, and nature of the agreement as a whole has to be taken into account³⁸³. Prof. Maresceau also summarises that direct effect ‘[...] is not some abstract characteristic which is found to exist or be lacking in isolation from the substance of the case’³⁸⁴. In other words, there cannot be room for abstract speculations on the direct effect of an agreement's dispositions, this should be assessed on a case-by-case-basis.

We should recall that the CJEU has been quite reticent in recognising direct effect, except for the jurisprudence developed on the basis of the GATT. In *International Fruit Company*³⁸⁵, the CJEU ruled that direct effect was the result of discussions held by the parties during the negotiations around the creation of the agreements, which should have been reflected therein: ‘[...] some negotiated agreement on reciprocity of direct effect would appear to be a *conditio sine qua non* for accepting the direct effect of GATT/WTO provisions’³⁸⁶. As Prof. Maresceau

³⁸⁰ Beth A. Simmons, “Compliance with international agreements”, *Annual Review Political Science*, No. 1, 1998, pp. 75-93, pp. 77-78.

³⁸¹ Marc Maresceau, 2004, *op. cit.*, p. 294.

³⁸² Similarly, Prof. Cannizzaro, 2012, *op. cit.*, pp. 35-58, p. 38, suggests that the direct effect of a treaty's provisions may be deduced from its clear, precise and consistent wording – as it is internally granted to EU directives – or because of ‘[...] the international nature of the provision and the purpose assigned to it in the international legal order from which it emanates’. See also C-104/81, *Hauptzollamt Mainz v C.A. Kupferberg & Cie KG a.A.*, 26 October 1982, EU:C:1982:362.

³⁸³ It should not be discarded, indeed, the possibility that the treaty itself set forth the legal effect of its provisions. See Marc Maresceau, 2004, *op. cit.*, pp. 247 and 248.

³⁸⁴ *Ibid.*, p. 248.

³⁸⁵ C-21 to 24/72, *International Fruit Company NV and others v Produktschap voor Groenten en Fruit*, 12 December 1972, EU:C:1972:115, and C-149/96, *Portuguese Republic v Council of the European Union*, 23 November 1999, EU:C:1999:574.

³⁸⁶ Marc Maresceau, *op. cit.*, p. 294.

observes: ‘The directed consequence of the *International Fruit Company* ruling was indeed that the Community was “liberated” from potential continuous judicial review of a substantial part of its domestic legislation in the light of GATT obligations, not only by the Court of Justice but, perhaps more importantly, also by national courts in the Member States’³⁸⁷. This was not the case in the GATT Agreements as far as the dispute settlement mechanism was concerned, since it was ‘[...] clear that the objective of WTO agreements is governing relationship between States or regional organizations and not to protect individuals’³⁸⁸.

In its subsequent jurisprudence³⁸⁹, the CJEU denied that direct effect may have been assumed if the EU had not adopted any internal legislation. Notably, in *Merck Genéricos* the Court highlighted that the lack of direct effect dispositions – specifically, Article 33 TRIPS – was compensated for by the fact that national courts were required to interpret national law consistently with the TRIPS³⁹⁰. Therefore, national judges may disapply domestic rules in conformity with international law: this practice has been renamed as “indirect effect”³⁹¹. In the judgment on the Aarhus Convention³⁹², for example, the CJEU ruled that Article 9(3) of the Aarhus Convention imposes on national authorities the duty to put administrative and judicial proceedings at the service of environmental interest, but this could have not been called for by individuals – i.e., it had no direct effect. However, national judges were finally obliged to disapply domestic rules and to recognise the *locus standi* to NGOs³⁹³. Prof. Fajardo del Castillo notes that the CJEU’s position might have left it open to challenge in the light of the consistency of the EU legal order, as the lack of bottom-down common procedures may have induced Member States to adopt different positions according to their interests³⁹⁴. However, it shall be recalled that when the CJEU refrains from providing direct effect to an *ad hoc* disposition, it may decide to deliver its own interpretation which finally mitigates the possibility of a

³⁸⁷ *Ibid.*, p. 248.

³⁸⁸ *Ibid.*, p. 294.

³⁸⁹ See also: C-70/8, *Fédération de l'industrie de l'huilerie de la CEE (Fediol) v Commission of the European Communities*, and C-69/89, *Nakajima v Council of the European Communities*; C-53/96, *Hermès International (a partnership limited by shares) and FHT Marketing Choice BV*, and C-337/95, *Parfums Christian Dior SA and Parfums Christian Dior BV and Evora BV*; C-149/96, *Portuguese Republic v Council of the European Union*, and the analysis of Piet Eeckhout, 2012, *op. cit.*, pp. 323-350.

³⁹⁰ C-431/05, *Merck Genéricos – Produtos Farmacêuticos Lda v Merck & Co. Inc.*, para. 48.

³⁹¹ Jan Willem Van Rossem, *op. cit.*, p. 67; Giacomo Gattinara, “Consistent Interpretation of WTO Rulings in the EU Legal Order?”, in Enzo Cannizzaro, Paolo Palchetti, and Ramses A Wessel, *op. cit.*, pp. 269-290, and Federico Casolari, “Giving Indirect Effect to International Law: The Doctrine of Consistent Interpretation”, in Enzo Cannizzaro, Paolo Palchetti, and Ramses A Wessel, *op. cit.*, pp. 395-416.

³⁹² C-240/09, *Lesoochránárske zoskupenie VLK v Ministerstvo životného prostredia Slovenskej republiky*, para. 50.

³⁹³ Marc Amstutz, “In between worlds: Marleasing and the emergence of interlegality in legal reasoning”, *European Law Journal*, No. 6, Vol. 11, 2005, pp. 766-784, p. 76.

³⁹⁴ Teresa Fajardo del Castillo, 2013, *op. cit.*, pp. 14, 15, and p. 23.

fragmented implementation³⁹⁵. Prof. Cannizzaro elucidates that from the CJEU's jurisprudence on direct effect at least three main elements are relevant: first, reciprocity; second, the existence of a dispute-settlement mechanisms, and finally, the granting of rights to individuals.

Regarding reciprocity, this requisite normally pushes the CJEU to exclude direct effect as it reduces the contracting parties' margin of manoeuvre when choosing the instrument of implementation³⁹⁶. Moreover, the CJEU admits that when one of the contracting parties only recognises the direct effect to a disposition, 'imbalanced obligations'³⁹⁷ may become problematic since it leads to different forms of interpretation and implementation³⁹⁸.

As far as mechanisms for the settlement of disputes are concerned, the author underlines that whether they are agreed or not does not impact the effect of the treaty³⁹⁹. In this regard, the CJEU found that the flexibility of the provision concerning the dispute settlement mechanism set forth by the GATT deprived its dispositions of legal effect⁴⁰⁰. Conversely, the WTO Agreements that foresaw a compulsory dispute settlement mechanism suggested to the CJEU that the parties aimed at keeping enforcement at the interstate level and, consequently, that it had no direct effect⁴⁰¹. Such a mechanism was estimated to be the right *forum* to litigate, but also that it was one of many, which prevents the establishment of any direct effect⁴⁰².

Direct effect dispositions that confer rights to individuals⁴⁰³ are especially interesting for our research since they enable them to challenge the validity of EU secondary law in national

³⁹⁵ C-53/96, *Hermès International (a partnership limited by shares) and FHT Marketing Choice BV*, paras. 32-33, and Eleftheria Neframi, 2012, "Mixed Agreements as a source of European Union Law", *op. cit.*, p. 334: '[...] the parameter of competence is not decisive in the framework of enforcement proceedings or in the case of substantive interpretation of a provision of a mixed agreement'.

³⁹⁶ Enzo Cannizzaro, 2012, *op. cit.*, p. 42. To be noted that Prof. Cannizzaro interpretes reciprocity not merely as a tool for compliance but as a part of the legal commitment the parties had entered into, whose content shall be determined dynamically on the basis of 'the mutual adjustment between the positions of the parties'.

³⁹⁷ C-104/81, *Hauptzollamt Mainz v C.A. Kupferberg & Cie KG a.A.*, para. 18.

³⁹⁸ C-21 to 24/72, *International Fruit Company NV and others v Produktschap voor Groenten en Fruit*, para 45.

³⁹⁹ See, for example, C-469/93, *Amministrazione delle Finanze dello Stato v. Chiquita Italia*, 12 December 1995, EU:C:1995:435, and Beatrice I. Bonafé, "Direct effect of International Agreements in the EU Legal Order: Does it Depend on the Existence of an International Dispute Settlement Mechanism?", in Enzo Cannizzaro, Paolo Palchetti, and Ramses A Wessel, *op. cit.*, pp. 229-28.

⁴⁰⁰ C-21 to 24/72, *International Fruit Company NV and others v Produktschap voor Groenten en Fruit*, para. 27.

⁴⁰¹ C-268/94, *Portuguese Republic v Council of the European Union*, 3 December 1996, EU:C:1996:461. See Antonello Tancredi, "On the Absence of Direct Effect of the WTO Dispute Settlement Body's Decisions in the EU Legal Order," in Enzo Cannizzaro, Paolo Palchetti, and Ramses A Wessel, *op. cit.*, pp. 249-268.

⁴⁰² Enzo Cannizzaro, 2012, *op. cit.*, pp. 44 and 45.

⁴⁰³ See: C-265/03, *Simutenkov v Ministerio de Educación y Cultura and Others*, 12 April 2005, EU:C:2005:213; C-344/04, *The queen, on the application of International Air Transport Association (IATA) and European Low Fares Airline Association (ELFAA), v. Department of Transport* 2006, and C-308/06, *The Queen, on the application of International Association of Independent Tanker Owners (Intertanko) and Others v Secretary of State for Transport*.

courts⁴⁰⁴. Winter recalls the Permanent Court of International Justice's judgment *La Grand*⁴⁰⁵ to highlight that an individual may invoke the dispositions of a treaty that create rights and obligations. This interpretation is supported by Prof. Eeckhout, who defines the Court's attitude since *Intertanko*⁴⁰⁶ as evidence of the EU's openness toward international law and, specifically, to the growing role of the individual in international law, which means that the right-to-freedoms test will occupy a prominent role in future jurisprudence⁴⁰⁷.

3.1.3. From horizontal to vertical enforcement

The regime through which states react to enforce international obligations in case of non-compliance is regulated by the International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts of 2001⁴⁰⁸ (DARS) that was coupled with another Draft Articles for International Organisations in 2011⁴⁰⁹ (DARIO). According to Tomuschat:

‘[...] any issue of responsibility starts out with an international commitment being encroached upon. This simple consideration applies to [international organisations] in the same way as it applies to States. If no conduct contrary to a rule of international law can be observed, the question on how to ensure respect of international law notwithstanding an act of non-respect simply does not arise’⁴¹⁰.

⁴⁰⁴ It is probably this introspection that spurs Thomas Buergenthal, *loc. cit.*, to talk about ‘direct applicability’ instead of ‘direct effect’. Yet, by doing so, the author stresses the existence of another major principle regulating the interrelationship between the EU and the Member States’ legal orders and, consequently, the international agreements concluded by the former, that is, the principle of primacy of EU law. The author also points out that the CJEU is cautious when it comes to apply EU principles to third parties, being these not bound by its interpretation.

⁴⁰⁵ ICJ, Judgment, *La Grand (Germany v USA)*, 2001, ICJ Rep. 466, recognising the right of the sending state to challenge at Court the infringement of the rights of a detained alien in the under the aegis of diplomatic protection.

⁴⁰⁶ C-308/06, *The Queen, on the application of International Association of Independent Tanker Owners (Intertanko) and Others v Secretary of State for Transport*.

⁴⁰⁷ Piet Eeckhout, 2012, *op. cit.*, pp. 381-383.

⁴⁰⁸ Resolution of the UN General Assembly No. A/RES/56/83 of 28 January 2002, *Responsibility of States for internationally wrongful acts*.

⁴⁰⁹ International Law Commission No. 10 (A/56/10) of 10 August 2001, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, available at www.legal.un.org. Only the DARS is considered to codify customary international law and general principles of law and, therefore, its rule bind the EU by virtue of Article 3(5) TEU – see Eleftheria Neframi, “Customary International Law and Article 3(5) TEU”, in Piet Eeckhout and Manuel Lopez Escudero, *op. cit.*, pp. 205-222, p. 210: ‘[...] while the conclusion of an international agreement by the Union embodies both an obligation to respect and a duty to implement, it is this latter duty that specifically stems from the exercise of a transferred competence, while the obligation to respect shows the subordination of the Union to the international law of treaties and this to customary international law’. The author highlights that, different from international agreements, customary international law is not a source of European law because it does not correspond to any underlying competence. The DARIO, instead, promotes the ‘progressive development’ rather than codification of existing practice – see Christine M. Chinkin, “United Nations Accountability for Violations of International Human Rights Law”, *The Hague Academy of International Law*, Vol. 395, 2018, pp. 199-320, p. 239.

⁴¹⁰ Christian Tomuschat, “The International Responsibility of the European Union”, in Enzo Cannizzaro, *op. cit.*, p. 180.

The regime on the responsibility of states and international organisations comprises two features: a ‘breach of an international obligation’ and the attribution of the ‘wrongful act’ under international law⁴¹¹. The DARIO specifies that the attribution as to who, or what, is the originator of the wrongful act is developed, as far as the member states of an international organisation are concerned, by the theory of control⁴¹². In the case of the EU ‘[...] as the Community is in a position to guarantee the Member States’ respect of the agreement by means of Community procedures. Consequently, if a Member States’ act violates a provision falling within the Member States’ area of competence, not only is the Member State at fault, but the Community can also be held responsible’⁴¹³. As far as the objective element is concerned, the wrongfulness, or not, of an act should be evaluated on the basis of the ‘international legal obligation binding such an entity’⁴¹⁴ instead, that is, by pointing out the category of obligations required⁴¹⁵, distinguishing *ius cogens* norms from general international law sources, as well as from conventional obligations⁴¹⁶.

⁴¹¹ Article 4 DARIO. Marjorie Beaulay, “Human Rights Protection and the Notion of Responsibility: Some Considerations About the European Case Law on State’s Activities under U.N. Charter”, in Norman WeißJean and Marc Thouvenin, *The Influence of Human Rights on International Law*, Cham, Springer, 2015, pp. 93-110, recalls that under international human rights law, the subjective element of ‘attribution’ must be read in the light of the principle of jurisdiction, while taking into account both its geographical or individual’s scopes.

⁴¹² A crucial contribution on the establishment of the responsibility of international organisations came from the ECtHR jurisprudence that, before the non-participation of the EU to the ECHR, had to resolve the delicate issue of the Member States’ responsibility for violations caused to individuals in the application of EU law. With *Bosphorus hava yollari turizm ve ticaret anonim şirketi v Ireland*, the ECtHR affirmed the EU offers a level of human rights protection *prima facie* equivalent to the one ensured by the ECHR. The favourable treatment reserved to the EU was justified by the CJEU’s willingness to follow up the ECtHR jurisprudence while enforcing EU law. Furthermore, the ECtHR jurisprudence on the UN peacekeeping operations specified that the attribution to an international organisation of the conduct of agents or organs of one of its Member State may occur in case the conduct of the agents/organs is under the “effective control” of the international organisation – *Behrami and Behrami v France, and Saramati v France, Germany and Norway* [GC], No. 71412/01 and No. 78166/01, 2 May 2007, CE:ECHR:2007:0502DEC007141201. In the frame of the UN peacekeeping operations, the ECtHR looks at the person holding the ‘direct operational command’ in a mission launched by the UN Security Council decision – Giorgio Gaja, “Responsabilité des états et/ou des organisations internationales en cas de violations des droits de l’homme: la question de l’attribution”, in Ronny Abraham, *Le droit international des droits de l’homme applicable aux activités des organisations internationales*, Paris, A. Pedone, 2009, pp. 95-103. This doctrine is sealed under Article 7 DARIO.

⁴¹³ Eleftheria Neframi, 2012, *op. cit.*, p. 202, and Article 7 DARIO recalling the theory on the ‘effective control’ for which: ‘The conduct of an organ of a State or an organ or agent of an international organization that is placed at the disposal of another international organization shall be considered under international law an act of the latter organization if the organization exercises effective control over that conduct’.

⁴¹⁴ Riccardo Pisillo Mazzeschi, *op. cit.*, p. 192: ‘[...] for the purposes of state responsibility, the really useful distinctions should not be made between different categories of rights, but rather between different categories of obligations’ (our own translation). The author also specifies that in the field of international human rights, the ‘wrongfulness’ of an injurious act is implicitly assumed in case of breach of the underlying international obligation, although it does not prejudice another State directly but the individual. See also Marjorie Beaulay, *op. cit.*, p. 101.

⁴¹⁵ Riccardo Pisillo Mazzeschi, *op. cit.*, p. 243, refers to the tripartite obligations to respect, protect, and fulfil and, among the latter, the obligation to facilitate, provide, and promote.

⁴¹⁶ Allan Rosas, “International Responsibility of the EU and the European Court of Justice”, in Malcolm Evans and Panos Koutrakos, *The international responsibility of the European Union*, Oregon, Hart Publishing, 2013, pp. 139-261, and Helena Torroja Mateu, *op. cit.*, p. 218.

However, the Vienna Convention on the Law of Treaties of 23 May 1969 neither regulates the protection of individuals ‘in terms of rights and obligations’⁴¹⁷, nor concerns itself with multilateral treaties that, especially in the human rights field, are directed at regulating ‘[...] the defence of the common interests of mankind’ or ‘growing global solidarity’⁴¹⁸. A small hint of the peculiarities of human rights treaties can be extracted from Article 60(5) of the Vienna Convention on the Law of Treaties of 23 May 1969 according to which, while derogating from the general principle of *inadimplenti non est adimplendum*, a material breach of a treaty does not allow the other contracting party to suspend or terminate the agreement if the provision violated relates ‘[...] to the protection of the human person contained in treaties of a humanitarian character, in particular to provisions prohibiting any form of reprisals against persons protected by such treaties’. It is expected that other states will extend their co-operation to put an end to such a breach and regard non-recognition of the obligation as unlawful, and that any aid or assistance granted to the violating state would also be unlawful⁴¹⁹. Prof. Meron highlights that this norm takes on board the integral nature of the obligations assumed by the states with human rights treaties for which ‘[...] any bilateral measure of reciprocal non-application would necessarily infringe upon the rights of all other states parties to continue the performance’⁴²⁰.

The development of *erga omnes* or *erga omnes partes*⁴²¹ obligations went hand in hand with the verticalisation – or institutionalisation – of international law. The verticalisation of the enforcement of international law has developed within universal or regional human rights regimes through two main phenomena: first, the provision of bodies of control, whether jurisdictional or not, within the international organisations (the bottom-down approach); and

⁴¹⁷ Meron Theodor, “International Law in the Age of Human Rights”, *Collected Courses of the Hague Academy of International Law*, Vol. 301, 2003, pp. 9-490, p. 186.

⁴¹⁸ *Ibid.*, pp. 186 and 187, and the authors *ivi* cited.

⁴¹⁹ Olivier de Schutter, *International Human Rights Law*, Cambridge, Cambridge University Press, 2017, p. 111, and Felix Ermacora, “Human Rights and Domestic Jurisdiction”, *Collected Courses of The Hague Academy of International Law*, Vol. 124, 1968, pp. 371-452, pp. 407-408.

⁴²⁰ *Ibid.*, pp. 211-212. See also Dinah Shelton, *Remedies in international human rights law*, Oxford, Oxford University Press, 2015, p. 58 ff., p. 59: ‘Human rights obligations differ from other areas of international law where treaty and customary obligations generally are reciprocal and treaty partners confer equal benefits on each other and accept equal duties in return [...] human rights obligations have the ‘purpose of guaranteeing the enjoyment of individual human beings of those rights and freedoms rather than to establish reciprocal relations between States’.

⁴²¹ Juan Antonio Carrillo Salcedo, 2001, p. 101, recalls (our own translation):

‘these agreements are [...] multilateral normative agreements in which the contractual dimension of treaties is attenuated to the extent that the conventional regulation goes beyond the reciprocity of rights and duties between States parties, since they seek the achievement of a common interest rather than the satisfaction of individual interests. But the principle of the consent of States as the basis and foundation of their treaty obligations does not disappear [...]’

second, the growing role of the individual in public international law (the bottom-up approach).

According to Prof. Picone:

‘As a result of the emergence of *erga omnes* obligations, the international legal system now finds itself «benefiting» from a «channel» for implementing the fundamental and/or absolute values of the international community, which operates in competition with, if not as an alternative to, the traditional channel constituted by the United Nations. These two channels «coexist», with no possibility of being institutionally «framed» in pre-established hierarchical positions of supremacy or subordination: but they are by their nature destined to enter into continuous reciprocal relations’⁴²².

The ICCPR’s system exemplifies the increasing importance played by international organisations in the enforcement of human rights, which compensates for the general lack of action by the international community and compulsory judicial settlement given that the state-centric enforcement approach has been progressively abandoned⁴²³. However, the gradual erosion of the states’ domestic jurisdiction regarding the protection of human rights⁴²⁴ has made them adopt crucial safeguards to preserve their primary role, among which the principle of subsidiarity stands out⁴²⁵. In addition, and as is the case regarding the right to privacy, states subjugate the protection of human rights to exception or derogation clauses in order to ‘[...] achieve a proper balance in favor of individual rights [with] reasonable necessities of States’ – e.g., to safeguard public order interests⁴²⁶. The prevailing use of soft enforcement mechanisms by human rights treaties – e.g., the Human Rights Committee in the case of the ICCPR – leads them to being ‘[...] considered ‘softened’, ‘defused’, or ‘decoupled’ from the body of general international law, with the result that the only means of securing compliance with human rights treaty obligations would be the machinery, if any, embodied in or attached to those treaties themselves’⁴²⁷. As a result, the enforceability of the ICCPR has been categorised as ‘impossible, primarily for political reasons, originating from [different national] and cultural perspectives on the application of Article 17 ICCPR and the HRC guidelines’⁴²⁸.

⁴²² Paolo Picone, *Comunità internazionale e obblighi «erga omnes»*, Napoli, Jovene Editore, 2013, p. 519 ff. (our own translation).

⁴²³ Meron Theodor, *op. cit.*, pp. 275-276, and A. Cançado Trindade, “Mechanisms of International Protection”, *Collected Courses of the Hague Academy of International Law*, Vol. 202, 1987, pp. 9-435, pp. 43-57.

⁴²⁴ A. Cançado Trindade, *op. cit.*, p. 34 ff.

⁴²⁵ *Ibid.*, p. 39 ff.

⁴²⁶ *Ibid.*, p. 40, which differentiates those rights from those formulated in absolute terms as analysed by the author p. 75 ff., and those having an imperative character examined p. 86 ff.

⁴²⁷ Bruno Simma and Philip Alston, “The sources of human rights law: custom, jus cogens, and general principles”, *Australian Yearbook of International Law*, pp. 82-108, p. 84.

⁴²⁸ Joanna Kulesza, “International law challenges to location privacy protection”, *International Data Privacy Law*, 2013, Vol. 3, No. 3, pp. 158-169, p. 161.

The Council of Europe system instead empowers individuals and gives them a leading role *vis-à-vis* states and the international community as a whole. Unlike other multilateral human rights treaties, the ECHR is not directed, or rather not firstly directed, at regulating inter-state reciprocal obligations, but at protecting the individual against any infringement perpetrated by the contracting parties⁴²⁹. Conversely, the Convention 108 is a ‘high-level instrument’⁴³⁰, and is clearly not enforceable *vis-à-vis* individuals provided that it has not been implemented in the domestic legal order⁴³¹. The Explanatory Memorandum to Convention 108 clarifies that each contracting party is free to implement its dispositions into domestic law so as to achieve the purposes and settle down the principles agreed therein. A step toward vertical enforcement was made with Convention 108+ that introduced soft forms of monitoring its implementation for which it ‘can be supplemented with more detailed soft-law sectoral texts in the form notably of Committee of Ministers’ recommendations elaborated with the participation of interested stakeholders’⁴³². Besides, the modernised Convention inserts a presumption of non-adequacy in case the contracting party has not implemented the Convention’s dispositions into its national law or has not generally observed such rights and obligations. However, the enforceability of Convention 108+ is still weak if compared to the ECHR: on the one hand, it has been argued that the Council of Europe does not have sufficient resources to deploy a constant monitoring activity and, instead, it must rely on the states parties ‘to challenge the quality and effectiveness of another State’s law and practices’⁴³³; on the other hand, its vertical enforcement excludes any judicial apparatus the individual could rely on to challenge the state infringing Convention 108+’s norms. Hence, Article 14(1) of Convention 108+ provides for a disconnection clause⁴³⁴ to enable EU Members States not to transfer personal data to the other contracting parties if:

‘A Party may also do so if bound by harmonized rules of protection shared by States belonging to a regional international organization’⁴³⁵.

⁴²⁹ United Nations, *Compilation of General Comments and General Recommendations Adopted by the Human Rights Treaty Bodies*, HRI/GEN/Rev.5, 26 April 2001, p. 150, para. 17.

⁴³⁰ Christopher Kuner, 2013, *op. cit.*, p. 37.

⁴³¹ According to it: ‘Each Party should take the necessary steps to give effect to this “common core” in its domestic legislation’ in the Explanatory Report to the Convention for the Protection of individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.01.1981, p. 5, available at www.rm.coe.int.

⁴³² *Ibidem*.

⁴³³ Christopher Kuner, 2013, *op. cit.*, p. 113.

⁴³⁴ Marise Cremona, “Disconnection Clauses in EU Law and Practices”, in Christophe Hillion and Panos Koutrakos, *op. cit.*, pp. 160-186. The author finds that the disconnection clause does not indicate the occurrence of the *AETR/ERTA* effect on common rules and it can be used indistinctively for shared and EU exclusive competences as well. What the clause really brings is transparency ‘[...] in making visible the obligations of the Member States as members of the EU as well as Parties to an international agreement’ (pp. 185-186).

⁴³⁵ Article 17(2), first paragraph, *in fine*, Convention 108+. It is important to note the French authorities’ position during the negotiations that stressed: ‘[...] if the EU Member States have to suspend their transfers of data to the other 17 States Parties to Convention 108 with which they have been exchanging data legally for years, while

However, while it is clear that this rule is necessary for those states that are not members of the Council of Europe, we believe that it should be revised for those that adhere to the ECHR. For these states, vertical bottom-up enforceability of Convention 108+ can be predicted as far as its norms are covered by Article 8 ECHR. This interpretation does not include those contracting parties that are not members of the ECHR – i.e., non-European states – as the individual falling under their jurisdiction could not challenge a breach of the Convention 108+ before the ECHR. Of course, if third countries are states of the Council of Europe, the system of human rights guaranteed by the latter is a subsidiary one *vis-à-vis* domestic constitutional systems. However, the international enforceability of Article 8 of the ECHR cannot be questioned provided that the ECHR is also empowered to assume complaints if the Member State concerned does not comply with its obligations, or in case there are insufficient remedies in the domestic order.

3.2. Enforcement in the data protection field

In the data protection field, bottom-up enforceability takes on different shapes in light of the numerous norms, parties, and institutions that are involved in this subject⁴³⁶. According to Prof. Hijmans:

‘Organisations processing personal data should know what they have to do to protect these fundamental rights and should be given the right incentives to protect, individuals should be given the right tools to protect themselves and the DPAs should be sufficiently empowered to play their role’⁴³⁷.

A systemic-teleological interpretation of the EU *acquis* on personal data suggests that the co-legislators aimed at ensuring the existence of data subject rights and effective legal remedies in case personal data was transferred to a third country⁴³⁸. Both the GDPR and the LED specify, as far as appropriate safeguards are concerned – including international treaties – that ‘[...] a

waiting for those States to adopt the EU's legislation or to have an adequacy decision granted, there is a risk that the process of adopting adequacy decisions will be slowed down considerably and that data transfers with those third States will be suspended for a long time’. Confront the Council of the EU, *Recommendation for a Council Decision authorising the opening of negotiations on the modernisation of Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (EST 108) and the conditions and modalities of accession of the European Union to the modernised Convention*, 6176/13 DCL 1, 30 January 2019, p.15.

⁴³⁶ Hielke Hijmans, 2016, *op. cit.*, pp. 157-188, finds that the transborder data flow regulation is an example of a pluralistic legal framework because the different stakeholders participating in it prevents from fitting in into a single regulatory theory.

⁴³⁷ *Ibid.*, p. 179.

⁴³⁸ Article 46(1) GDPR: ‘In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available’.

controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available⁴³⁹. Thus, the term “enforceability” gives effectiveness to the individuals’ rights according to the domestic legal orders of the contracting parties. Unlike enforceability, effectiveness measures how Member States adapt their behaviour to fall in line with the commitments or dispositions adopted within a specific regime⁴⁴⁰. In his dissertation, Prof. Hilmans finds that effectiveness is directed at ‘[...] ensuring that the general principles of privacy and data protection are translated into protection of the individual in practice’⁴⁴¹. According to the author, effectiveness is an imperative requisite set forth under Article 16(1) TFEU, and Articles 7 and 8 of the CFREU, and compels the EU to ensure that they are respected even in horizontal relations between private parties. Specifically, effectiveness shall be ensured by: the judicial control exercised by the CJEU, the legislation adopted under Article 16(2) TFEU, and the control developed by the supervisory authority. Svantesson, for his part, summarises that enforceability is triggered by supervisory authorities and by individuals to which we are addressing⁴⁴².

3.2.1. The role of independent supervisory authorities

In *European Commission v Federal Republic of Germany*, the CJEU maintained that:

‘[...] supervisory authorities must ensure a fair balance between, on the one hand, respect for the fundamental right to private life and, on the other hand, the interests which require the free movement of personal data’⁴⁴³.

⁴³⁹ Article 46(1) GDPR. This is not the case of the LED whose Article 37(1)(a) only refer to ‘legally binding instrument’ without further specifications. Moreover, the LED does not regulate the possibility that the transfer of information is channelled through an administrative arrangement either.

⁴⁴⁰ N. Cornago Proeto, “Elementos para el análisis del proceso político en los regímenes internacionales: el multilateralismo no necesariamente formalizado”, *Anuario Español de Derecho Internacional*, Vol. 15, 1999, pp. 205-234, p. 228 (our own translation):

‘The problem of compliance with commitments should not be confused with that of the effectiveness of the regime in question. An effective international regime is in place when States adapt their behaviour to the commitments or provisions adopted within the regime in question. If, after laborious negotiations, states have established a system of quotas on crude oil exports, whaling, or the launching of satellites into orbit, the regime will have been effective if states effectively comply with their commitments. The effectiveness of the regime does not necessarily presume the existence of control or sanction systems, although these may sometimes be necessary. Effectiveness is simply judged on the basis of the fulfilment of the behavioural expectations’.

⁴⁴¹ Hielke Hilmans, 2016, *op. cit.*, pp. 125-183, p. 174.

⁴⁴² Dan Svantesson, 2016, *op. cit.*, pp. 195-222.

⁴⁴³ C-518/07, *European Commission v Federal Republic of Germany*, 9 March 2010, EU:C:2010:125, para. 24. Article 51(1) GDPR confirms that independent supervisory authorities support both the protection and the free movement of personal data. Yet, Hielke Hilmans, 2020, “Article 51: Supervisory authority”, in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *op. cit.*, pp. 863-872, p. 868, considers questionable the fact that Article

Independent supervisory authorities monitor the consistent application of EU law in all Member States and, in this regard, support the European Commission in its main role as the guardian of the founding Treaties. In practice, independent supervisory authorities are called on to cooperate with the European Commission without losing their independent position for which they are granted a hybrid position within the institutions: they are represented within the EDPB together with the EDPS. The latter deploys the same supervisory functions at the central level⁴⁴⁴ and, consequently, monitors the activities of EU agencies among which are the Europol, the European Public Prosecutor⁴⁴⁵ (EPPO), and the Eurojust⁴⁴⁶ and it oversees a cooperation mechanism in the fields of large-scale IT systems⁴⁴⁷.

At the national level, independent supervisory authorities are part of the mechanism of remedies guaranteed to natural persons for the protection of their personal data and, as such, they may exercise investigative powers⁴⁴⁸ if they receive a complaint from an individual and, where necessary, may also become involved in legal processing⁴⁴⁹. Each supervisory authority has a limited territorial competence that is based upon three main criteria⁴⁵⁰, namely:

- the controller or processor is established in the territory of the Member State of the supervisory authority;
- data subjects residing in the Member State of the supervisory authority are substantially affected, or likely to be substantially affected, by the processing, or
- a complaint has been lodged with the supervisory authority.

51(2) GDPR includes a mandate to monitor the facilitation of the free flow of data in the Member States since on the one hand, this reference does not take into account the change of emphasis on EU data protection following the entry into force of the Lisbon Treaty and, from the other one, the reference to the free flow of data is linked to the two overarching objectives of the GDPR, Article 1(1).

⁴⁴⁴ Note that the EDPS' decisions may be submitted directly to the CJEU according to Articles 58(4) and 64 of EUDPR.

⁴⁴⁵ Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), *OJ L 283*, 31.10.2017, pp. 1-7 (EPPO Regulation hereinafter).

⁴⁴⁶ Article 62 EUDPR.

⁴⁴⁷ Article 61(1) EUDPR.

⁴⁴⁸ Article 58(1) GDPR

⁴⁴⁹ See Article 57 GDPR, point (f), specifying that supervisory authorities '[...] shall process complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and outcome of the investigation within a reasonable time, in particular whether it is necessary to further investigate or coordinate with another supervisory authority'. The European Commission has proposed to use the Internal Market Information System to allow the exchange information between competent national authorities, the European Commission and other Union bodies, offices, and agencies with the added participation of the EDPS and the EDPB – see the Opinion of the EDPS No. 8/2017 on the *proposal for a Regulation establishing a single digital gateway and the 'once-only' principle*, Brussels, 1.08.2017, p. 16 ff.

⁴⁵⁰ Article 58 GDPR.

Their tasks are not limited to a supervisory function, but include the enforcement of data protection provisions⁴⁵¹. Supervisory authorities may use a range of instruments that range from hard to soft measures that often make use of the “stick and carrot” technique, where the stick is largely comprised of sanctions⁴⁵² and the carrot of incentives⁴⁵³. In *Weltimmo*, for example, the CJEU analysed whether the Hungarian data protection authority could have imposed a fine on a data protection controller employed by a company registered in Slovakia that was processing the data of advertisers that had previously published sales lists for their Hungarian properties in *Weltimmo*’s website, even after they had submitted an erasure request⁴⁵⁴. The CJEU found that *Weltimmo* was exercising its activity in Hungary and not in Slovakia and therefore the Hungarian national supervisory authority could neither have exercised its executive powers in Slovakia, nor could it have issued any penalty. The CJEU affirmed that when the supervisory authority receiving a complaint concludes that it cannot impose penalties outside the territory of its own Member State, ‘[...] it must, in fulfilment of the duty of cooperation laid down in Article 28(6) of that directive, request the supervisory authority of that other Member State to establish an infringement of that law and to impose penalties if that law permits, based, where necessary, on the information which the authority of the first Member State has transmitted to the authority of that other Member State’⁴⁵⁵. In other words, and given that each supervisory authority has a limited territorial competence, they are obliged to cooperate with each other in cases of transborder breaches of personal data.

⁴⁵¹ See the EDPB, *Toolbox on essential data protection safeguards for enforcement cooperation between EEA data protection authorities and competent data protection authorities of third countries*, Brussels, 14.03.2022, and the EDPB, *Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities*, Brussels, 5.08.2021.

⁴⁵² See Article 83 GDPR: while this provision provides for specific sums of money depending on the infringement, the legislator has left Member States to establish specific rules in the public sector. In any case, fines shall be ‘effective, proportionate and dissuasive’. The EDPS may impose fines from 50.000 to 500.000 euros to the EU Institutions and bodies.

⁴⁵³ For example, an effective carrot law measure is the ‘naming and shaming’ that in public international law usually consists in ‘reputational consequences of noncompliant behaviour’ as explained by Beth A. Simmons, *op. cit.*, pp. 77-78, p. 81.

⁴⁵⁴ C-230/14, *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1 October 2015, EU:C:2015:639.

⁴⁵⁵ *Ibid.*, paras 56 and 57. See also C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, where the Wirtschaftsakademie asked if the German supervisory authority could have exercised the powers of Article 28(3) DPD before an establishment that was exercising its advertising space and other marketing activities within its territory, while the processing of personal data was undertaken by an establishment located in another Member States and having the main establishment was placed outside the EU. The CJEU found that Facebook Germany to be an establishment whose activity – namely the promotion and sale activities – were intrinsically linked to the data processing activity developed in the Facebook webpage. Therefore, the German supervisory authority could have evaluated the lawfulness of the processing of personal data conducted by a third party established in another Member State shall in full autonomy, without prejudice of the cooperative mechanism set forth under Article 28(6) DPD.

When the processing of the data is performed by public authorities, national supervisory authorities are exclusively competent⁴⁵⁶ even though the data processing has a cross-border dimension⁴⁵⁷. In this sense, public authorities are always monitored by their own supervisory authority and the mechanisms of the lead supervisory authority do not apply. The supervisory authority may fall back on the mutual assistance and joint data protection mechanisms offered by the national authority⁴⁵⁸. This exemption is also extended to ‘public service missions’, that is, private undertakings subject to a legal obligation or operating in the public interest. For example, in case of the transfer of PNR data by an air carrier, the competent data protection authority is that of the Member State in which the flight landed or departed from⁴⁵⁹.

Another important derogation to the jurisdiction principle of the territoriality of supervisory authorities is the one-stop-shop mechanism that enables the individual to address a sole supervisory authority if the data processing activity concerning him/her affects several Member States⁴⁶⁰. The one-stop-shop mechanism has been inserted to overcome the reticence of national governments in centralising the enforcement of the EU data protection law while coordinating their activities between one another⁴⁶¹. According to Prof. De Hert:

‘If a data controller conducts cross-border data processing in the EU, according to the GDPR the supervisory authority is the one based in the Member State where the data controller has its main establishment. If the data controller’s activity concerns citizens of another Member States, the local DPA of that state may hand over the case to the DPA of the main establishment (lead supervisory authority) or can handle the case locally in co-operation with the latter’⁴⁶².

The one-stop-shop mechanism regulates the allocation of competences between a ‘lead supervisory authority’ and the other supervisory authorities concerned⁴⁶³. Such a mechanism ensures that several supervisory authorities must cooperate in cases of transborder data processing activities and, lastly compels them to reach a consensus and a joint decision, which is binding on all those authorities and with which the controller must ensure compliance as regards processing activities undertaken in the context of all its establishments within the EU⁴⁶⁴. According to the CJEU:

⁴⁵⁶ Article 6(1)(c) and (e) GDPR

⁴⁵⁷ Article 55(2) GDPR.

⁴⁵⁸ *Ibidem*.

⁴⁵⁹ See Article 8 of the PNR Directive.

⁴⁶⁰ Articles 55-56 GDPR.

⁴⁶¹ Which could have been achieved by establishing a single European agency or supervisory structure, as advanced by the Belgian data protection authority and by Paul De Hert, 2021, *op. cit.*, p. 312 ff.

⁴⁶² *Ibid.*, p. 306.

⁴⁶³ C-645/19, *Facebook Belgium BVBA v Gegevensbeschermingsautoriteit*, 15 June 2021, EU:C:2021:483, para. 50.

⁴⁶⁴ *Ibid.*, para. 52.

‘The application of the ‘one-stop shop’ mechanism consequently requires, as confirmed in recital 13 of Regulation 2016/679, sincere and effective cooperation between the lead supervisory authority and the other supervisory authorities concerned’⁴⁶⁵.

In cases of disagreement between the lead supervisory authority and one or more data protection authorities, the former should submit the case to the EDPB to obtain a binding decision⁴⁶⁶. Only in exceptional circumstances will the GDPR allow another supervisory authority other than the lead authority to issue a decision, these conditions include: if the subject matter relates only to an establishment in its own Member State or substantially affects data subjects in that Member State alone⁴⁶⁷, and in case of an urgent procedure⁴⁶⁸. The CJEU ruled that any decision taken by supervisory authorities other than the lead one would jeopardise the objective and effectiveness of such a cooperative procedure⁴⁶⁹.

Transborder cooperation between Member States’ administrative authorities enforces data protection rules across the EU across a number of areas, including: the realisation of trainings and financial resources; the provision of domestic legal mandate/authority to accomplish program implementation, as well as the access to relevant information⁴⁷⁰. Article 50 GDPR foresees that the administrative cooperation in the data protection field should reach foreign territories too, and, specifically, it seeks to:

- set up ‘international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data’;
- provide for international mutual assistance mechanisms to enforce the legislation for the protection of personal data;
- involve relevant stakeholders in discussions and activities, and
- exchange and document personal data protection legislation and practice, particularly in case of jurisdictional conflicts with third countries.

As Hustinx recalls, the combination of the regime on the transfer of personal data set forth by the EU data protection *acquis*, together with the cooperation of national supervisory authorities:

‘[...] will facilitate a gradual development towards global ‘interoperability’ of privacy and data protection frameworks. Although it would be fairly easy to identify many differences in terms of detail, there is also a growing scope for synergy and convergence among those frameworks. The [GDPR] would be the most developed framework in the world—line with the recognition. Of the right to data protection as fundamental right in

⁴⁶⁵ *Ibid.*, para. 53.

⁴⁶⁶ Article 63 GDPR.

⁴⁶⁷ Article 58 GDPR.

⁴⁶⁸ Article 66 GDPR.

⁴⁶⁹ C-645/19, *Facebook Belgium BVBA v Gegevensbeschermingsautoriteit*, para. 65.

⁴⁷⁰ Beth A. Simmons, *op. cit.*, p. 83.

Article 8 of the Charter—but it would also be consistent with developments elsewhere. Moreover, it may well have a strong influence on those developments in due course, much like Directive 95/46/EC exercised in the past. The review of the Directive therefore also offer[ed] a major opportunity to ensure more global privacy and interoperability⁴⁷¹.

Thus, supervisory authorities are in charge of ensuring the enforceability of individuals' rights in case of transborder flows of data, playing the role of an "intermediary" and effectively allowing the individuals to attend court.

3.2.2. The effective protection of individuals' rights

The EU data protection *acquis* empowers the individual to defend his/her data protection rights by establishing that the individual shall be granted 'enforceable' rights consisting of the rights to access, to rectification, to erasure, to restriction of processing, and to object to data processing activities, despite the fact that these rights can be restricted⁴⁷². The data subject should be able to lodge a complaint and to access a judicial remedy in the light of Article 47 of the CFREU, especially in case of non-action by the data controller so that a breach of the data protection principles enshrined in Articles 6 and 7 GDPR must always ensure a direct access to national courts by the individual⁴⁷³. The GDPR reformulates this in the following terms:

'Without prejudice to available administrative or non-judicial remedies, including the right to lodge a complaint with a supervisory authority [...] every data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in breach of this Regulation'⁴⁷⁴.

Similarly, Article 54 LED provides that the data subject is to be granted the right to lodge a complaint with a supervisory authority, or to seek a judicial remedy when the right to access to and rectify personal data is restricted. Such a guarantee is also ensured in through the one-stop-shop mechanism if the lead supervisory authority does not provide for mutual assistance where another supervisory authority is concerned. According to the CJEU, the latter could adopt a provisional measure or, after consulting the EDPB, a final binding one in cases of urgency. Afterwards, '[...] the supervisory authority concerned must be able to take the necessary measures to ensure compliance with the rules on the protection of the rights of natural persons as regards the processing of personal data contained in Regulation 2016/679 and, for that

⁴⁷¹ Peter Hustinx, 2017, *op. cit.*, p. 165.

⁴⁷² See Chapter I.

⁴⁷³ C-465/00, C-138/01 and C-139/01, *Rundfunk*, 20 May 2003, EU:C:2003:294, para. 100: 'These provisions are sufficiently precise to be relied on by individuals and applied by national courts. Furthermore, while it is true that Directive 95/46 confers on the Member States a more or less wide discretion in the application of some of its provisions, Articles 6(1)(c) and 7(c) or (e) lay down unconditional obligations'.

⁴⁷⁴ Article 79 GDPR.

purpose, exercise the power conferred on it by Article 58(5) of that regulation'⁴⁷⁵, that is, the possibility to bring infringements to the attention of the judicial authorities and, if necessary, to institute or otherwise initiate legal proceedings with a view to ensuring compliance with its provisions.

The CJEU jurisprudence suggests that the right to a remedy may also be exercised before a non-judicial body, yet, in any case, the data protection authority shall be ensured access to justice⁴⁷⁶. Although Article 58(5) of the GDPR does not specify in what circumstances the national supervisory authorities may initiate or engage in legal proceedings, '[...] it is sufficient that the supervisory authority should have the possibility, in accordance with national legislation, to bring to the attention of the judicial authorities infringements of that regulation and, where appropriate, to initiate or engage in legal proceedings or to commence, in some other manner, a procedure for the enforcement of the provisions of that regulation'⁴⁷⁷. The CJEU observed that such a power could be exercised with respect to the main establishment of the controller located in that authority's own Member State, as well as with respect to another of the controller's establishments located outside the authority's territory 'provided that the object of the legal proceedings is a processing of data carried out in the context of the activities of that establishment and that that authority is competent to exercise that power'⁴⁷⁸. Also, it found that although Facebook's main establishment was located in Ireland and the branch located in Belgium was created, primarily, to allow the Facebook group to engage with the EU institutions and, secondly, to promote the advertising and marketing of that group to people residing in Belgium, the activities carried out by the latter 'must be considered to be inextricably linked to the processing of personal data at issue in the main proceedings' though only the former was the controller within the EU. In these terms, the Court advanced the possibility that the activities of Facebook in Belgium could be considered as being carried out 'in the context of the activities of an establishment of a controller', as stated within Article 3(1) of the GDPR.

Until recently, it was not clear whether consultation with the national supervisory authority was an indispensable preliminary step in order to access justice. Article 22 DPD formulated in general terms that Member States should ensure the right to an effective judicial remedy to challenge any breach individuals may suffer in case of a breach of the data protection law.

⁴⁷⁵ C-645/19, *Facebook Belgium BVBA v Gegevensbeschermingsautoriteit*, para. 71.

⁴⁷⁶ See Chapter I.

⁴⁷⁷ C-645/19, *Facebook Belgium BVBA v Gegevensbeschermingsautoriteit*, para. 112.

⁴⁷⁸ *Ibid.*, para. 96.

When analysing the former Article 22 of the DPD⁴⁷⁹, Prof. Brouwer claimed that Member States could have insisted upon prior referral to the supervisory authority as a prerequisite for exercising the individual's right to an effective remedy before the national judicial authority⁴⁸⁰. Provided that the ability of data protection authorities to bring infringements before judicial authorities depends on national law and on the legal procedure ensuring the application of the GDPR⁴⁸¹ – recalling that supervisory authorities may impose administrative fines and penalties on processors and controllers⁴⁸² –, direct or indirect access to the national court is regulated by each national legal system. However, it was already clear from the DPFD that the right to an effective remedy could have been exercised without prejudice to the administrative remedy⁴⁸³.

In *Puškár*⁴⁸⁴, the CJEU clarified that the provision of exhaustion of available administrative remedies is not prohibited *per se*, but inevitably constitutes an obstacle to the right to an effective remedy. Therefore, Article 47 read in conjunction with Article 52(1) of the CFREU, provides that such a restriction must be established by law, in full respect of the essence of those rights and the principle of proportionality, if it is necessary to effectively achieve an objective of general interest recognised by the EU, or if there is a need to protect the rights and freedoms of others⁴⁸⁵. In this sense, the prior exhaustion of administrative remedies should not lead to a substantial delay in bringing legal action⁴⁸⁶. Moreover, the CJEU clarified that:

‘[...] although, in principle, Member States may impose an appropriate fee for bringing an action before an administrative authority, that fee cannot, however, be set at a level which could constitute an obstacle to the exercise of the right to a judicial remedy guaranteed by Article 47 of the Charter. In that regard, account must be taken of the fact that that fee is added to the costs of the judicial proceedings’⁴⁸⁷.

⁴⁷⁹ According to which: ‘Without prejudice to administrative remedies which may be available, in particular: before the supervisory authority referred to in Article 28, Member States shall, before bringing the matter before the judicial authority, provide for the right of every person to a judicial remedy in the event of a breach of the rights guaranteed to him or her by the national law applicable to the processing in question’.

⁴⁸⁰ See Evelien Brouwer, *Digital borders and real rights: Effective remedies for third-country nationals in the Schengen Information System*, Boston, Martinus Nijhoff Publishers, 2008, p. 232.

⁴⁸¹ See Article 58(5) GDPR.

⁴⁸² See Article 84 GDPR.

⁴⁸³ ‘Without prejudice to any administrative remedy which may be provided for prior to referral to the judicial authority, the data subject shall have the right to a judicial remedy in the event of a breach of the rights guaranteed to him by the applicable national law’.

⁴⁸⁴ C-73/16, *Peter Puškár v Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy*.

⁴⁸⁵ In *Puškár*, *ibid.*, the CJEU argued that there was a certain degree of uncertainty as to when the time limit for bringing an action before the national court started if an administrative authority had taken an earlier decision. This would prevent access to judicial protection and would be contrary to Article 47.

⁴⁸⁶ Hielke Hijmans, 2016, *op. cit.*, pp. 335-336, maintains that in the multi-layered structure of remedies set forth by virtue of Article 16 TFEU, the remedy before the data protection authority is alternative to the one brought before the national court.

⁴⁸⁷ C-73/16, *Peter Puškár v Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy*, para. 75.

Consequently, national supervisory authorities are part of the chain of remedies comprising the right to effective judicial protection in the light of Articles 7, 8, and 47 of the CFREU. In this sense, they also serve to control and balance the rule of law when public actors are under their control⁴⁸⁸. Indeed, when access to the judicial authority is not granted, then, the presence of an independent authority plays a prominent role not only *ex post facto* but also *ex ante*. As Advocate General Mengozzi said:

‘[...] the fact that the agreement envisaged has failed to provide that access by the authorised officials of the CBSA to the PNR data is subject to prior control by an independent administrative authority or by a court is not incompatible with Articles 7 and 8 and Article 52(1) of the Charter, in so far as — as is the case — the agreement envisaged requires that Canada guarantee that every person concerned will be entitled to an effective post factum judicial review of the decisions or actions relating to access to his PNR data’⁴⁸⁹.

What the GDPR still does not clarify is whether data protection authorities are obliged to investigate when the data subject makes a complaint under Article 77⁴⁹⁰ GDPR and, if they are obliged, if any inactivity may be challenged before a court or tribunal, however, this has been clarified in the framework regarding the transfer of personal data.

First, in *Maximillian Schrems v Data Protection Commissioner*⁴⁹¹, the CJEU found that the adoption of an adequate decision could not limit the right to lodge a claim before the competent national supervisory authority, nor could the powers of the latter be limited by the sole fact that the European Commission adopted such a decision. As a result, in cases where an individual’s claim put into question the existence of appropriate safeguards with regard to the protection of personal data, the national supervisory authority should fully and independently evaluate whether the transfer of personal data to a third country is deemed to be lawful despite the Commission’s assessment. If the national supervisory authority finds that claim is unfounded, the data subject shall be granted access to a judicial remedy in the light of Article 47 of the

⁴⁸⁸ Some resource, human and financial problems may undermine the effectiveness of the data protection authorities’ action – see Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU approach to the digital transition — two years of application of the General Data Protection Regulation, COM(2020) 264 final, Brussels, 24.6.2020.

⁴⁸⁹ Opinion of Advocate General Mengozzi, *Opinion 1/15*, para. 272.

⁴⁹⁰ For which:

‘1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in his or her Member State of habitual residence, place of work or place of the alleged infringement, if he or she considers that the processing of personal data relating to him or her infringes this Regulation. 2. The supervisory authority to which the complaint has been lodged shall inform the complainant of the progress and outcome of the complaint, including the possibility of judicial redress in accordance with Article 78’.

This question has been raised in C-192/15, *Rease and Wullems*, of 9 December 2015, EU:C:2015:861, and the CJEU will therefore have to determine the legality of the refusal of the Dutch data protection authority to investigate Rease’s and Wullems’ complaint on the basis that the alleged infringement was not sufficiently serious.

⁴⁹¹ See C-362/14, *Maximillian Schrems v Data Protection Commissioner*.

CFREU. Otherwise, if claim is well founded, the national supervisory authority itself shall be given the chance to access national courts, so that the latter may submit a preliminary ruling request to the CJEU on the validity of the Commission's decision.

Second, in *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*, the CJEU was asked whether the national supervisory authority should prevent the transfer of data from a Member State to a third country in case the adequacy level of protection was sealed by a Commission's decision validating Standard Contractual Clauses⁴⁹². As the new GDPR expressly establishes, national supervisory authorities have to suspend or prohibit the transfer of personal data to a third country if the standard data protection clauses are not, or cannot be, complied with in the third country and if the protection of the data transferred as required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended, or put an end to, the transfer⁴⁹³. The High Court observed that the adoption of Standard Contractual Clauses in no way limits the national supervisory authorities' powers. However, it also added that, before the binding nature of decisions implemented by the Commission, Member States' and their bodies should comply with the European Commission's adequacy decision until it is declared invalid. In practice, when receiving a complaint by an individual alleging that the transfer of data toward a third country does not ensure the *continuum* of the protection of fundamental rights as required by EU law, then, national supervisory authorities should examine it by means of their investigative power and, eventually, bring an action before the national Court. However, it has already been pointed out that each national supervisory authority can exercise its investigatory powers within the territory of the Member State it belongs to. As a result, in cases of the transfer of personal data to a third country or

⁴⁹² See C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*, paras. 109 and 110. According to Article 93(2) GDPR as well as the Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, *OJ* L181, 04.07.2001, pp. 19-31, the Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, *OJ* L 385, 29.12.2004, pp. 74-84, and the Commission Decision 2010/87 of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, *OJ* L 39, 12.2.2010, pp. 5-18. It can be advanced that the European Commission proposed on 12 November 2020 to revise this model by proposing new ones in the Commission Implementing Decision (EU) .../... on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, and its relevant Annex. This had been revised by the EDPB – see the Joint Opinion of the EDPS-EDPB No. 2/2021 on *the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries for the matters referred to in Article 46(2)(c) of Regulation (EU) 2016/679*, Brussels, 14.01.2021.

⁴⁹³ Article 58(2)(f) and (j) GDPR.

organisation, procedural guarantees enabling the cooperation between EU and foreign supervisory authorities must be agreed.

All in all, the major difficulty to overcome in cases of the transfer of personal data to a foreign country or international organisation is triggered by the need for extraterritorial enforceability. As Prof. Kuner highlights, while adequacy purports to provide a strong level of protection for personal data, such protection is difficult to enforce outside the borders of the EU. The author then suggests concentrating accountability standards on the transferring authority that falls under EU law, as this is the only solution practical, workable solution, i.e., the granting of a remedy against a data exporter in the complainant's own country⁴⁹⁴. In Prof. Kuner's words, the data subject shall be empowered to exercise his/her rights before the transferring authority within EU law only to avoid transborder enforceability problems. Nevertheless, this is not the position assumed by the CJEU when it established in its jurisprudence that individuals shall also be granted effective legal remedies before a tribunal in a foreign country⁴⁹⁵. In pursuit of the ruling – and while admitting that the form of the instrument does not ensure *per se* its binding nature or enforceability – the EDPB suggests incorporating express data protection provisions in the agreement enabling the transfer of personal data or the addition of a further annex in order to ensure the availability of judicial redress. Otherwise, the EDPB recommends⁴⁹⁶ the effective application of data protection principles on both sides and, in case of non-judicial readdress, it suggests consulting the competent supervisory authority before agreeing an alternative readdress mechanism.

4. The revision of existing international agreements

Article 96 GDPR regulates the compatibility of international agreements concluded by the Member States before their adoption. According to it:

‘International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked’.

⁴⁹⁴ Christopher Kuner, 2009, *op. cit.*, p. 271.

⁴⁹⁵ *Opinion 1/15*, paras. 220, 226, and 227.

⁴⁹⁶ Guidelines of the EDPS No. 2/2020 on articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies, Brussels, 15.12.2020.

This “grandfather clause” was strongly supported by the Member States during the negotiations of the GDPR⁴⁹⁷. Similarly, Article 61 LED provides for the regulation of previous international agreements and is worded as follows:

‘International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 6 May 2016 and which comply with Union law as applicable prior to that date shall remain in force until amended, replaced or revoked’.

As the French delegation noted during the negotiations, this norm would have obliged the Member States to align their international agreements with third countries⁴⁹⁸, including bilateral and multilateral agreements concluded, for example, in the fields of law enforcement, judicial, financial, tax and customs. Although in the 2012 Proposal competent authorities were pointed out as being responsible for the amendment of previously concluded international agreements if this was deemed necessary⁴⁹⁹, the Article 29 DPWP supported the position of the European Commission and of the European Parliament, that pushed for the introduction of an obligation to amend these treaties so as to ensure ‘at the very least’ their compliance in the light of the EU *acquis*⁵⁰⁰. The EDPS, for its part, was the main body arguing for prohibiting the conclusion of bilateral agreements during the transposition period, it also complained about the lack of a provision for a time-limit that would compel Member States to amend international agreements already in force, which was not finally incorporated⁵⁰¹.

⁴⁹⁷ See the French position in Council of the EU, 6723/13, Brussels, 26 February 2013 (04.03), p. 41.

⁴⁹⁸ Council of the EU, 6846/14 ADD 1, Brussels, 25 February 2014 (28.02), p. 4.

⁴⁹⁹ Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, Brussels, 25.1.2012, Article 60. This clause would have demanded the Member States to denounce existing international agreements and to re-negotiate the, only in case of necessity. As the French delegation highlighted, denouncing a treaty may be tough especially in the short time initially envisaged in Council of the EU, 6846/14 ADD 1, Brussels, 25 February 2014 (28.02), p. 3:

‘As is probably the case for a lot of other Member States, France has a large number of bilateral agreements in the areas of police, judicial, financial, tax and customs cooperation. Renegotiating these agreements would lead to increased requirements in terms of equipment and personnel [...] There are also many multilateral agreements on information and data exchange within the context of police, judicial, financial, tax and customs activities which would be covered by Article 60. These would have to be denounced by all the Member States of the EU, entailing highly complex and not necessarily feasible renegotiations’.

Hence, the revision of existing international agreements should be conducted by the own Member States in a flexible way.

⁵⁰⁰ Opinion of the EDPS No. 03/2015 on *the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, Brussels, 1.12.2015, p. 16.

⁵⁰¹ Opinion of the EDPS No. 6/2015, *A further step towards comprehensive EU data protection. EDPS recommendations on the Directive for data protection in the police and justice sectors*, Brussels, 28.10.2015, p. 9.

Article 96 GDPR and 61 LED do not specify whether it is the duty of the EU or the Member States, or both, to make ‘amendments, replacements, or revocations’ to international agreements, however, the theory on implied external competence comes in our support. Discarding the possibility that the EU has acquired an external exclusive competence by virtue of Article 16(2) TFEU⁵⁰², it is up to the Member States and/or the EU to amend, replace or revoke the agreements in question. In case the EU acts, this could invoke its competence by virtue of the principle of subsidiarity as far as this complies with Union law applicable prior to that date, though Member States may impose their co-presence in the negotiations and ratification process while opting for the mixed formula. Otherwise, Member States may continue concluding international treaties provided that these do not impose more stringent rules than the LED, so as to leave the EU free to raise the degree of internal harmonisation in the future.

The EDPB stressed the need to revise Member States’ international agreements on the transfer of personal data to third countries and organisations⁵⁰³, as well as sectoral agreements concerning tax purposes, social security, mutual legal assistance, police cooperation, and so on. According to the EDPB: ‘This review should be done in order to determine whether, while pursuing the important public interests covered by the agreements, further alignment with current Union legislation and case law on data protection, as well as EDPB guidance might be needed’⁵⁰⁴. The EDPB invited Member States to follow its guidelines and it committed to issuing more instructions covering agreements concluded in the fields covered by the LED⁵⁰⁵.

In any case, Article 96 GDPR does not address cases where agreements concluded by the Member State are ‘incompatible’ with previously existing data protection legislation – that is the DPD – and *a fortiori* with the current data protection package. It can be recalled that, in case of ‘substantial incompatibility’, Article 351 TFEU establishes that:

⁵⁰² Hielke Hijmans, 2016, *op. cit.*, p. 449 ff., Marise Cremona, 2012, *op. cit.*, p. 315, and Paula García Andrade, 2015, *op. cit.*, p. 205 ff. Article 59 of the Vienna Convention on the Law of Treaties of 23 May 1969 provides that as soon as the same parties conclude a new treaty with the same subject-matter the previous one shall be considered as terminated. When new agreements, or clauses thereto, are concluded by the EU only under its exclusive competence, scholars consider that Member States are ‘third parties improperly’ which means that they are third parties in the Treaty but not before the international organisation they belong to – Sobrino Heredia and Rey Aneiros, “Las relaciones entre los Estados Partes en un tratado celebrado por una Organización Internacional y los Estados miembros de ésta”, in Mariño Menéndez, *El Derecho Internacional en los albores del siglo XXI? Homenaje al Profesor Juan Manuel Castro-Rial Canosa*, Trotta, Madrid, 2002, pp. 559-638, p. 635 ff. In this sense the substitution of an agreement between a Member State and a third country by an agreement conclude between the latter and the EU it’s possible by virtue of the competence Member States transfer to the EU in order to celebrate the international agreement – Paula García Andrade, 2015, *op. cit.*, p. 209.

⁵⁰³ See the Letter of the EDPB to the European Parliament, Brussels, 7.06.2021, available at www.edpb.europa.eu.

⁵⁰⁴ Statement of the EDPS No. 04/2021 on *international agreements including transfers*, Brussels, 13.04.2021.

⁵⁰⁵ Confront the Work Programme of the EDPB No. 2021/2022, Brussels, 16 March 2021.

‘To the extent that [the agreements concluded before 1 January 1958 or, for acceding States] are not compatible with the Treaties, the Member State or States concerned shall take all appropriate steps to eliminate the incompatibilities established’⁵⁰⁶.

If they did not take appropriate steps, the Member States would remain in the uncomfortable position of infringing on their international commitments, or EU law⁵⁰⁷. However, although an incompatible agreement is considered to be provisionally valid, Member States are called upon to eliminate discrepancies between the international agreement and EU law. As a result, Member States shall interpret the agreement in conformity with EU law, renegotiate the agreement or, as a last resort, denounce the treaty if it is permissible under public international law in order to conform their international agreements with EU law. Yet, Article 351 TFEU is not applicable to agreements other than those concluded before 1 January 1958, or those concluded before the Member State joined the EU. For example, it is not extendable to treaties concluded by the Member States after their accession if a shared competence exists between the EU and its Member States⁵⁰⁸. A threshold may be established by the founding principles of EU law under the terms explained by Prof. Eeckhout, who highlights that Article 351 TFEU ‘[...] could not be understood to authorize any derogation from the principles of liberty, democracy, and respect for human rights and fundamental freedoms enshrined in (then) Article 6(1) EU (currently reflected in Article 2 TEU)’⁵⁰⁹. Recalling the *Kadi*⁵¹⁰ judgment, the author highlights that the CJEU established the EU to be a *sui generis* legal order where the protection of fundamental rights always prevails:

‘According to this case law, EU concepts on fundamental rights prevail, whenever this is necessary, over international law. EU law contains principles that must be respected in the international domain, are not negotiable and subject to full review of the EU Courts’⁵¹¹.

⁵⁰⁶ It shall be noted that Paula García Andrade, 2015, *loc. cit.*, extends the interpretation of Article 351 TFEU – and with it, the provision of a transitory period in which the Member State’s agreement would not be challengeable against EU law – to the agreements concluded after 1 January 1958 or after the accession but before the conferral of new competence to the EU sealed under the revision of the foundational treaties. Conversely, this reasoning should not be applicable after the new allocation of competence has been agreed but before the EU would have made use of it. *A fortiori*, this reasoning is applicable to the data protection field where the EU grabs a new competence by virtue of Article 100a of the 1992 TEC. Following her path, Member States could not know that the (then) European Community would have occupied such a subject so that the agreement concluded before the DPD entered into force should have remained valid for a transitory period. Yet, as soon as the European Commission made its proposal, Member States should have refrained from undertaking international negotiations.

⁵⁰⁷ Paula García Andrade, 2015, *op. cit.*, p. 212. In case the denounce would not be feasible according to Article 56 of the Vienna Convention on the Law of Treaties of 23 May 1969, then, the author underlines that the state will surely be called to respond of its international responsibility.

⁵⁰⁸ Opinion of Advocate General Capotorti, C-155/80, *Procureur Général v. Arbelaiz-Emazebe*, 27 May 1981, EU:C:1981:123, para 4.

⁵⁰⁹ Piet Eeckhout, 2012, *op. cit.*, p. 429.

⁵¹⁰ C-402/05 P and C-415/05 P, *Yassin Abdullah Kadi and Al Barakaat International Foundation*.

⁵¹¹ Hielke Hijmans, 2016, *op. cit.*, p. 473.

Therefore, in no case can Article 96 GDPR read in the light of Article 351 TFEU be interpreted as allowing Member States to derogate from the CFREU, although non-substantially incompatible agreements may be ‘tolerated’ until their amendment, replacement, or revocation. However, this interpretation raises further issues: first, the delimitation of the essential content of the fundamental rights to respect to a private and family life (Article 7 CFREU) and to the protection of personal data (Article 8 CFREU), which, to date, have not been defined clearly⁵¹²; second, the constitutional value of the CFREU in the Member States’ domestic legal orders, that is, its position in the hierarchy of sources of law, especially in systems where a domestic Bill of Rights would prevail. This rationale is also applicable to the agreements concluded by the EU. Recital (102) GDPR establishes that:

‘This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects’⁵¹³.

Such a clause infers that international agreements previously concluded by the EU that imply the transfer of personal data shall not be amended and aligned to the GDPR provisions⁵¹⁴. In such a circumstance, and in case the third country has not been issued an adequacy decision, the international agreement would still govern the transfer of personal data. Thus, public international law should prevail over EU law even, if the treaty were incompatible with EU law. Article 98 GDPR adds that:

‘The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data’⁵¹⁵.

These norms give absolute priority to the *pacta sunt servanda* principle while leaving the EU legislator great discretion when it comes to revising existing international agreements. Nevertheless, it should be recalled that international agreements concluded by the EU should always meet the higher principles and rules of the EU legal order, under penalty of invalidity which ‘[...] has then almost certainly potentially damaging effects in the relations with the third country and, for the Community, there might probably be no other way out than to ask the

⁵¹² See Chapter I.

⁵¹³ Recital (102), first sentence, GDPR.

⁵¹⁴ See the Greece comment wondering ‘What happens in the cases of bilateral agreements, i.e. concluded between EU Member States and third countries’ in Council of the EU, 6723/13, Brussels, 26 February 2013 (04.03), p. 16.

⁵¹⁵ Article 98 GDPR.

partner to re-open negotiations about the substance of the agreement’⁵¹⁶. In the case of the transfer of personal data special attention shall be given to the applicable limitations in light of Articles 8 and 52(1) of the CFREU and, among the various requirements listed therein, the strict necessity test stands out as was analysed our previous Chapter⁵¹⁷. Provided that these limitations stem from EU primary law, including the CFREU, they cannot invalidate any agreement according to public international law unless they concern rules of fundamental importance, and violations did in fact take place⁵¹⁸. It is up to the EU, then, to suspend and denounce or withdraw from the agreement if the commitment is not compatible with its constitutional order.

⁵¹⁶ Marc Maresceau, 2004, *op. cit.*, p. 244. The author highlights that if the CJEU concerns, instead, are directed to procedural or inter-institutional matters only – e.g., the allocation of competences and the choice of the correct legal basis – this shall not lead to the renegotiations of the agreements. It is suggested, indeed, that the Court maintains the legal effects of the Council decision concluding the agreement until the measures for the implementation of the judgment have been taken.

⁵¹⁷ See Chapter I.

⁵¹⁸ Article 46 of the Vienna Convention on the Law of Treaties of 23 May 1969. The concept of “fundamental rules” is subjected to different interpretations: some authors go back to constitutional provisions; others may claim other internal norms provided that their constitutions do not lay down treaty making rules – see Jan Klabbers, *op. cit.*, p. 173.

CHAPTER III

THE EUROPEAN UNION'S LARGE-SCALE FREEDOM, SECURITY AND JUSTICE IT SYSTEMS

Unlike domestic legal orders, where government regulates in the wake of the legislator by virtue of its executive power, the latter is split between different institutions in the EU according to the paramount principle of conferral¹. This principle implies that the EU is not conferred whatsoever with any powers of implementation beyond those underpinned by a concrete legal basis in the founding Treaties. Because of the race to integration experienced at the legislative level², Member States have always been reluctant to confer implementing powers to the EU and have, in fact, jealously guarded their operational capacity by virtue of the principle of indirect administration. Indirect administration prevents the EU from acting at the administrative level, notwithstanding the provision of a specific legal basis empowering it to adopt legislative measures, unless expressly stated otherwise.

Information networks are one of several facets in which the EU implements policies³. As Prof. Curtin and Prof. Brito Bastos highlight:

‘Networked information-sharing [...] represents an institutional choice that may help promote uniform implementation without resulting in far-reaching transfers of power to the EU’s own authorities. Indeed [...] Member States often only agree to the creation of new EU agencies once

¹ Pieter Jan Kuijper, “Case Law of the Court of Justice of the EU and the Allocation of External Relation Powers”, in Marise Cremona and Anne Thies, *op. cit.*, pp. 95-114, p. 101: ‘Thus, the Commission can be said to possess a mix of executive, legislative and even (quasi-) judicial powers’. CFSP apart, the author highlights that the European Commission co-executes the EU external action together with the Council and it has the monopoly on the external representation of the EU – Article 17(1) *in fine* of the TEU – the legislative initiative – Article 17(2) TEU and Article 294(2) of the TFEU –, and the infringement procedure – Article 258 TFEU.

² R. Daniel Kelemen, “European Union Agencies”, in Erik Jones, Anand Menon, and Stephen Weatherill, *The Oxford Handbook of the European Union*, Oxford, Oxford University Press, 2014, pp. 392-406, p. 396:

‘The Commission used the power and autonomy it was granted to aggrandize its power and accelerate integration beyond the scope intended by at least some of the member states. Member States worked to mitigate this loss of control beginning in the 1960s by building a system of intergovernmental “comitology” committees that monitor and to some degrees control the Commission’s exercise of its executive powers [...] However, when Member states block delegation to the Commission itself, the Commission may support the establishment of autonomous EU-level regulatory bodies. In that case it will favour the establishment of EU agencies with considerable autonomy from national governments, but which remain closely tied to and dependent on the European Commission’.

³ Herwig C. H. Hofmann, Gerard C. Rowe, and Alexander H. Türk, *Administrative law and policy of the European Union*, Oxford, Oxford University Press, 2013, p. 307 ff. The “core-shell” model of EU administrative law is made of: the European Commission (Articles 17-18 TEU, Article 244 ff. TFEU), Union agencies, and committees (Articles 291 TFEU). As for the latter, Eberhard Schmidt-Aßmann and Fruzsina Molnár-Gábor, “European Administrative Law”, in Anne Peters and Rüdiger Wolfrum, *Max Planck Encyclopedias of International Law*, 2019, available at www.opil-ouplaw.com, find that: ‘Alongside the regulatory agencies, the comitology committees are the second element of decentralized centrality, without which administration of the European Union territory would not be possible’.

information exchange has failed to produce desired outcomes of uniform and effective policy implementation⁴.

Large-scale IT systems support the exchange of information, including personal data, which contributes to the implementation of EU policies. However, their IT services appear to go beyond a simple channel for the trafficking of information. Recalling the European Commission's position during the SIS II negotiations:

'The current debate on the nature of the SIS will inevitably have an impact on the technical solution to be considered as there is a significant difference between, for example, a system that only forwards messages and one which would also handle queries from end-users, as some are suggesting'⁵.

In the absence of a specific empowerment on common computer systems containing personal data files⁶, large-scale IT systems have been developed on the basis of a specific EU policy and in response to the need to implement an *ad hoc* competence recognised to the EU by the Member States in the founding Treaties⁷. When referring to the Proposal for a Regulation concerning the VIS and the exchange of data regarding short-stay visas in our view, for example, the Council Legal Service warned that:

'If the institutions decide to establish such systems, they must refer to the provisions which empower the Community or the Union to organize forms of cooperation between the relevant departments in the Member States by means of exchange of information'⁸.

In the fields of borders, migration, and asylum the picture was complex as the founding Treaties provided the EU with substantive legal bases but a sole provision regulated the practical cooperation among Member States and among Member States and the European Commission. Thus, Article 74 TFEU became the key legal basis to establish large-scale IT systems, but the necessary twinning of substantial and practical legal bases was by the European Commission's preference for the use of a single competence. As for PJCCM competences, the

⁴ Deirdre Curtin and Filipe Brito Bastos, "Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue", *European Public Law*, Vol. 26, No. 1, 2020, pp. 59-70, p. 60.

⁵ See the Council of the EU, *Communication from the Commission to the Council and the European Parliament on development of the Schengen Information System II*, 5472/02, Brussels, 29 January 2002, p. 10.

⁶ See *infra*.

⁷ See Didier Bigo, Sergio Carrera, Ben Hayes, Nicholas Hernanz, and Julien Jeandesboz, "Justice and Home Affairs Databases and a Smart Borders System at EU External Borders: An Evaluation of Current and Forthcoming Proposals", *Centre of European Policies Studies*, No. 52, December 2012, p. 14: '[t]here is undeniably a link between specific data and information exchange schemes and policy areas'. The authors take the example of the Eurodac to recall that its main function is related to the implementation of the EU's asylum policy, and the one of the VIS as far as the visa policy is concerned. Also, in C-43/12, *European Commission v European Parliament and the Council*, 6 May 2014, EU:C:2014:298, the CJEU supported the European Commission's pretension for which the appropriate legal basis of Directive 2011/82/EU of the European Parliament and of the Council of 25 October 2011 facilitating the cross-border exchange of information on road safety related traffic offences, OJ L 288, 5.11.2011, pp. 1-15, was Article 91(1) TFEU in spite of Article 87(2) TFEU.

⁸ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas - Legal basis*, 6683/05, Brussels, 23 February 2005, p. 5.

establishment of new systems was apparently not problematic, as the range of the EU legal bases in this area was specifically devised at the cooperative-operational level, regarding both law enforcement and judicial authorities.

Since the '90s, large-scale IT systems have undergone several reforms due to an unprecedented technological revolution, but they have also kneeled before political choices taken by the co-legislators. Thus, numerous authorities and freedom, security, and justice agencies have been granted access to these systems, notwithstanding the policy that underpins their respective competences and mandates, this raises questions about the paramount principle of purpose limitation as far as the processing of personal data is concerned⁹. For this reason, centralised databases have been severely criticised for their 'adaptable, flexible and dynamic nature'¹⁰. Even if large-scale IT systems are increasingly covered with data protection rules, there is still considerable reluctance to use Article 16 TFEU as the appropriate legal basis to side with the correspondent freedom, security and justice competence. Large-scale IT systems are perceived as tools enhancing the practical cooperation between national and Union agencies so as to execute freedom, security and justice objectives. However, this interpretation has been gradually losing support among EU institutions and, specifically, the EDPS has repeatedly emphasised the need to include Article 16 TFEU as the correct legal basis underpinning for regulations on large-scale IT systems.

This Chapter explores the possibility of finding a definition for a large-scale IT system of the AFSJ to highlight their added value as a cooperative tool. To achieve this, we will explore different information exchange models used as part of other EU policies to enhance inter-agencies cooperation. Afterwards, the research scrutinises the evolution of the EU's six existing large-scale IT systems in the light of the new central role played by the processing of personal data and the EU data protection *acquis*. This exploration will show that freedom, security and justice agencies' access to large-scale IT systems, notwithstanding the underlying policy field, blurs their original policy-centred nature and, consequently, flexes the principle of conferral, which represents the very basis of their implementation. In order to address these critical issues, we argue that Article 16 TFEU should be inserted as the correct legal basis alongside the AFSJ competences upon which large-scale IT systems are developed.

⁹ See Chapter I.

¹⁰ Niovi Vavoula, "Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?", *European Public Law*, Vol. 26, No. 1, 2020, pp. 131-156, p. 135.

1. Large-scale IT systems enhancing inter-agency cooperation

Different classifications of information exchange models have been advanced as part of the EU's composite administration¹¹ where the decisions must be taken in unison in order to enhance reciprocal trust¹². We believe that a major distinction can be drawn to differentiate the data request model from other forms of spontaneous exchange of information among the Member States' administrative agencies.

The data request model includes the possibility to request information regardless of the existence of an underlying regulation. In this sense, Prof. Schneider highlights that the authority to which the request has been made has no obligation to disclose the information since both authorities must proceed according to their domestic laws. A mutual mechanism for information exchange, instead, is based on the principle of reciprocity: here, the requesting authority *motu proprio* seeks the information from another authority on the basis of a previous commitment that obliges the latter to respond. Lafarge maintains that these mechanisms '[...] made it compulsory to any competent national administration to answer the requests made by any other competent national administration and to transmit it any information that may enable it to ensure compliance with the provisions of the relevant legislation'¹³. The author gathers both situations described above under the so-called 'single transmission mechanism' to highlight that, in these two cases, a prior request for information is needed.

Following this logic, Schneider points out that 'structured cooperation mechanisms' are based on sector-specific requirements and not on a general mutual assistance request. Although the author does not offer a clear overview of the categories of models included within the concept of 'structured cooperation mechanisms', the examples are presented on the assumption of the existence of a previous request and of a previous commitment – be it bilateral, multilateral, or institutionalised – which prevents the requested authority from interrupting the cooperative chain. Prof. Schneider suggests to systematise structured cooperation mechanisms after an organised model that includes: the duty of the requested authority to comply with a

¹¹ David Fernández Rojo, "El diseño de una administración supranacional e integrada para el espacio europeo de libertad, seguridad y justicia", *Revista General de Derecho Administrativo*, No. 58, 2021, pp. 1-40.

¹² Jean-Peter Schneider, "Information exchange and its problems", in Carol Harlow, Päivi Leino, and Giacinto della Cananea, *Research Handbook on EU Administrative Law*, Cheltenham/Northampton, Edward Elgar Publishing, 2017, pp. 81-112, points out four main categories of information exchange: upon request; through structured cooperation mechanism; spontaneous without prior request, and shared databases. François Lafarge, "Administrative Cooperation between Member States and Implementation of EU Law", *European Public Law*, No. 4, Vol. 16, 2010, pp. 597-616, instead, points out that information can be exchanged by different means among which: single transmission information; databases; single mutual information mechanism, and alert systems.

¹³ François Lafarge, *loc. cit.*

request for information by a specific deadline; the provision of predefined workflows for information exchange – e.g., common dictionaries or pre-translated questions and answers; the establishment of tracking mechanisms that allow the requesting authority to follow-up on its request; the agreement of predefined workflows for consensual problem solving, or the possibility of formulating a request not only in *ad hoc* cases concerning individuals, but also for groups of people, provided that such a request does not end up as a ‘fishing expedition’. In other words, a certain degree of organisation needs to exist so that the information is exchanged on the basis of previous requests through pre-convened communication channels. For example, the Smart Open Services for European patients implemented by Directive 2011/24/EU of the European Parliament and of the Council¹⁴ consists of a communication system through which a healthcare professional can request the information of a patient residing in another Member State through the so-called National Contact Point¹⁵.

The spontaneous model, instead, contemplates a duty imposed on an authority to transmit the information to another authority without prior request. According to Prof. Schneider, here the information is not gathered for another authority, but rather on the basis of the needs of the transmitting authority. The author finds this model especially relevant when covering shared administrative responsibilities within the EU. The first example given by the author is the one of an alert system the purpose of which is to ‘[...] facilitate the rapid exchange of information between Member States and the Commission on measures taken to prevent or restrict the marketing or use of products posing a serious risk to the health and safety of consumers’¹⁶. Consider, for example, the Early Warning and Response System set forth under Decision No 1082/2013/EU of the European Parliament and of the Council for which Member States and European Commission must issue an alert to combat serious cross-border threats to health¹⁷. Schneider depicts the automatic exchange of information as a second example of the spontaneous model. According to the author, automatic exchange consists of the periodic and systematic transmission of large volumes of predefined categories of recurring information, as is exemplified by the automatic exchange mechanism established to fight tax evasion and tax

¹⁴ Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients’ rights in cross-border healthcare, *OJ L* 88, 4.4.2011, pp. 45-65.

¹⁵ See the Working Document of the Article 29 DPWP No. 01/2012 on *epSOS*, Brussels, 25.01.2012.

¹⁶ Jean-Peter Schneider, *loc. cit.*

¹⁷ Article 8 of Decision 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC Text with EEA relevance, *OJ L* 293, 5.11.2013, pp. 1-15.

fraud¹⁸. Nevertheless, what Schneider seems to describe using the expression ‘automatic exchange of information’ is an automated procedure that periodically transmits huge amounts of personal data on the basis of a previous agreement between the authorities involved¹⁹. For its part, Lafarge recalls that mutual information mechanisms allow Member States to spontaneously exchange information, as is the case of Council Decision 2006/688/EC of 5 October 2006, by which national authorities are called upon to exchange information on asylum and immigration matters²⁰. In this case, the procedure is not automated as it is up to a human being to input the data and this is automatically transferred through a specific network. Unlike with manual operations, the automatic exchange of personal data raises huge concerns from a data protection perspective. According to the EDPS:

‘[a] centralized electronic system also creates certain risks. These include, most importantly, that more data might be shared and more broadly than strictly necessary for the purposes of efficient cooperation, and that data, including potentially outdated and inaccurate data, might remain in the electronic system longer than necessary [...]’²¹.

The establishment of shared databases can be perceived as a form of (automatic) information exchange, though Schneider separates it from the spontaneous model. According to the author, databases can be based on a structured information mechanism and/or a duty to inform. In these terms, it is difficult to trace a clear line between the information exchange model – with or without a prior request – and shared databases. Yet, the latter clearly brings something more, as Prof. Schneider notes:

‘The added value of shared databases, which raises specific legal questions, consists in the direct availability of the data for longer period of time and of options for the systematic retrieval of data, as well as the possibility of linking data from various sources entered into the database at various times and events’²².

¹⁸ See the Statement of the Article 29 DPWP on *automatic inter-state exchanges of personal data for tax purpose*, Brussels, 4.02.2015, evaluating the establishment of a system of automatic inter-state exchange of personal data for tax purposes.

¹⁹ While the word ‘automated’ describes the conversion of a system or facility so that it predominantly works with automatic equipment, the term ‘automatic’ describes the means through which the information is exchanged – i.e., the fact that it is self-generated, spontaneous, or self-acting so that it does not require (or requires little) human intervention. See Andrew Butterfield, Gerard Ekembe Ngond, and Anne Kerr, “automate, v.”, in Andrew Butterfield, Gerard Ekembe Ngond, and Anne Kerr, *A Dictionary of Computer Science*, Oxford, Oxford University Press, 2016, available at www.oed.com.

²⁰ Council Decision 2006/688/EC of 5 October 2006 on the establishment of a mutual information mechanism concerning Member States’ measures in the areas of asylum and immigration, *OJ L* 283, 14.10.2006, pp. 40-43.

²¹ See the Opinion of the EDPS on *the Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data (2008/49/EC)*, Brussels, 25.10.2008, para. 7. The Internal Market Information System has been established to support two directives, namely: Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, *OJ L* 376, 27.12.2006, pp. 36-68, and Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications (Text with EEA relevance), *OJ L* 255, 30.9.2005, pp. 22-142.

²² Jean-Peter Schneider, *op. cit.*, p. 93.

In our perspective, shared databases are distinct from all other forms of information exchange since, by allowing information to be available for a long period of time, they facilitate the organisation of information to resolve a given case²³. These proprieties make databases a unique tool of cooperation, not so much for the way in which the information is requested, accessed or shared among the participating states, but because of the modalities through which the answer is given. We believe that the prolonged availability of information should be interpreted as the constant automatic response given by other countries that did not input the data into the system. In these terms, centralised databases are useful not only to satisfy the unique needs of a requesting Member State – e.g., in the case of administrative collaboration for taxation purposes²⁴ – but also and, especially, to achieve common objectives as pursued in a decentralised administration. Shared databases avoid cooperation gaps that may exist in case of non-response from one participating State to another, so as to ensure the coordination of national authorities in decision-making processes. In other words, they ensure the most efficient channel for the information to flow among a group of states when one state's decision impacts on other states. For this reason, shared databases cannot fit into the strict interpretation of the “spontaneous model” given by Prof. Schneider provided that this is limited to unique needs – which, in any case, can also be questioned considering the case of the Early Warning and Response System²⁵. However, a wider interpretation of the spontaneous model, contemplating the achievement of common objectives, would enable the systematisation of shared databases under that definition.

Although personal data does not constitute the sole source of information that can be exchanged and stored in these databases, the development of centralised systems commonly shared among Member States has been achievable only thanks to the previous harmonisation of domestic laws on the protection of personal data. As Lafarge highlights:

‘[...] the setting up of European databases led to the creation of harmonized personal data processing principles at Community level. The main European legislation in the field, the Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, was adopted shortly after two of the more

²³ Usually known as CMS as we will see in Chapters V and VI.

²⁴ See Francesca Tassinari, 2021, “La transmisión de información fiscal frente a la Carta de Derechos Fundamentales: reflexiones sobre la Sentencia del Tribunal de Justicia de 6 de octubre de 2020, *État Luxembourgeois*”, *loc. cit.*

²⁵ Notably, in the specific case of information systems, including IT infrastructure, Jeans-Peter Schneider, *loc. cit.*, maintained that these would not constitute a category on its own but an ‘[...] hermeneutic umbrella for many different forms of integrated information management’. IT is the branch of technology concerned with the dissemination, processing, and storage of information, especially by means of computers – see Andrew Butterfield and John Szymanski, “information technology, n.”, in Andrew Butterfield and John Szymanski, *A Dictionary of Electronics and Electrical Engineering*, Oxford, Oxford University Press, 2018, available at www.oed.com.

important European databases processing personal data became operational, the SIS (March 1995) and the CIS (July 1995)’²⁶.

Unlike other forms of information exchange, databases have attracted the attention of academics precisely for the challenges they imply for the protection of personal data. Large-scale IT systems may be conceived as ‘big databases’ due to the volume and different types of information, including personal data, processed therein²⁷. Indeed, a first major characteristic shared by these large-scale IT systems is the impact they have on huge numbers of data subjects. Large-scale IT systems usually share an architectural template made of a Central System (C-S) and a National System (N-S) for each Member State. As a consequence, they are geographically extended so as to embrace the whole Schengen territory. The transmission of data from the N-S to the C-S, and vice versa, flows into the so-called Interface Control Document (ICD) that is held within the communication infrastructure, in other words, an *ad hoc* network allows the systems to communicate with each other. For this purpose, the communication infrastructure is equipped with the capacity to rapidly exchange a considerable volume of data through a secured channel.

Another common characteristic encountered when studying databases is the duration, or permanence, of the data stored therein: large-scale IT systems are data containers that store information for pre-established periods of time. In addition, the number and variety of authorities that are simultaneously granted access to the systems must be taken into account. Indeed, centralised systems facilitate access to the information by simply conferring new access rights to different categories of authorities, including those of the EU. Last but not least, large-scale IT systems have been progressively integrated with AI features enabling, for example, mutual automated cross-checking procedures²⁸ which convert them into new Intelligent Technology systems²⁹. This technical solution enables the exchange of information not only

²⁶ François Lafarge, *op. cit.*, p. 613. The author leaves unresolved some questions like:

‘How are the access points to the databases chosen? Is this a competence left to national governments? Do agreement procedures of the access points exist at national or European levels? Is there a justiciability of mismanagement of databases by national administrations (and in the case of databases, mismanagement is not limited to false information but extended to lack of information, inaccurate, or insufficient information)? Who checks and reviews these databases?’.

²⁷ See the definition of large-scale processing of personal data given by the Guidelines of the Article 29 DPWP on *Data Protection Officers* (‘DPOs’), Brussels, 13.12.2017, p. 7.

²⁸ Niovi Vavoula, “Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism”, *European Journal of Migration and Law*, Vol. 23, No. 4, 2021, pp. 457-484.

²⁹ Arguably, freedom, security, and justice large-scale IT systems have been excluded from the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM(2021) 206 final, Brussels, 21.4.2021. Its Article 83 establishes that:

‘This Regulation shall not apply to the AI systems which are components of the large-scale IT systems established by the legal acts listed in Annex IX that have been placed on the market or put into service before

among the Member States' administrations, but also between administrations and EU bodies and organisms or between the latter only. In this sense, centralised databases integrate the maximum degree of operational cooperation both horizontally and vertically.

2. Schengen Information System (SIS)

2.1. From the first to the second generation of the SIS

The 1990 Convention implementing the Schengen Agreement was accompanied by a list of compensatory or flanking measures that sought to remedy the lack of security due to the absence of controls at internal EU borders³⁰. A major achievement in this field was the implementation of the SIS that entered into force in 1998³¹.

The SIS experimented with the creation of a supranational database shared among a handful of Member States and allowed national authorities to centrally store information on persons and objects³². SIS is effectively the ancestor of all EU large-scale IT systems, and its centralised part (C-SIS) resulted from the interconnection of existing national databases (N-SIS). Still today, its peculiar configuration makes the SIS a particularly exceptional system: Member States are authorised to keep national copies of the alerts stored therein³³ and these are

[12 months after the date of application of this Regulation referred to in Article 85(2)], unless the replacement or amendment of those legal acts leads to a significant change in the design or intended purpose of the AI system or AI systems concerned. The requirements laid down in this Regulation shall be taken into account, where applicable, in the evaluation of each large-scale IT systems established by the legal acts listed in Annex IX to be undertaken as provided for in those respective acts. 2. This Regulation shall apply to the high-risk AI systems, other than the ones referred to in paragraph 1, that have been placed on the market or put into service before [date of application of this Regulation referred to in Article 85(2)], only if, from that date, those systems are subject to significant changes in their design or intended purpose’.

The EDPB and the EDPS complained about the European Commission Proposal and recommended: first, to clarify the meaning of significant changes in design or intended purposes; second, to apply the requirement to put AI systems into service from the date of application of the future Regulation. See the Joint Opinion of the EDPB-EDPS No. 5/2021 on *the proposal for a Regulation of the European parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act)*, Brussels, 18.06.2021, p. 13.

³⁰ See Anna Fiodorova, *Information Exchange and EU Law Enforcement*, London, Routledge, 2018, p. 25, who affirms that the ‘[a]bolishment of internal border controls and free movement of people and goods also meant the abolishment of obstacles and risks to moving criminal activities to other Member States, as well as allowing free circulation of criminals, either to commit crime or to hide from law enforcement and justice authorities of other Member States where crime had been committed’. On the Schengen Convention see Vincent Lecocq, “La convention de Schengen”, *Defense Nationale*, No. 3, 1992, pp. 91-99, and David O’Keeffe, *loc. cit.*

³¹ See Articles 92 to 119 of the Convention implementing the Schengen Agreement. Confront also the Decision of the Executive Committee on *a catch-all clause to cover the whole technical Schengen acquis*, SCH/Com-ex (98) 29 rev, Brussels, 23.06.1998.

³² On the SIS, see: Stephan Kabera Karanja, *Transparency and proportionality in the Schengen Information System and border control co-operation*, Leiden, Nijhoff, 2008; Evelien Brouwer, 2008, *op. cit.*, pp. 47-70, and Madeleine Colvin, “The Schengen information System: a human rights audit”, *European Human Rights Law Review*, No. 3, 2001, pp. 271-279.

³³ It shall be noted that at the very beginning it was not clear how national copies should have been distinguished by the national systems which raised serious concerns from a data protection perspective. See, among others, the

periodically transmitted to the central station through the interconnection facilitated by the National Interface³⁴. Thanks to the existence of this technical tool, national and central data files are identical.

The SIS works through the provision of alerts – i.e., instructions that one Member State sends to another one in order to undertake specific actions. The system contains different categories of alerts: few of them are related to the suppression of border controls, while the majority are related to cooperation in the law enforcement and criminal judicial fields. The information exchange among States is automatic through a hit/no-hit mechanism. Apart from the alerts, the SIS allows the exchange of information through the SIRENE Bureaux³⁵.

Since it was first put into motion, the SIS has passed through at least two main revisions that are presented below.

2.1.1. The communitarisation of the SIS

At the time of its integration under EU Law, the SIS was by nature an inter-pillar measure. The provisions of the Convention implementing the Schengen Agreement and which regulated the SIS were integrated in the 1997 TEC and the 1997 TEU – also known as a “ventilation procedure” – to cover the SIS provisions on:

- the administration of the system;
- the regulation of alerts regarding borders and law enforcement, and
- the provisions establishing data protection guarantees³⁶.

From that moment on, any measure developing the Schengen *acquis* should have been underpinned by the appropriate legal bases of the founding Treaties³⁷. The Greek template structure imposed by the Maastricht Treaty forced the EU to double the legislative measures under the first and third pillars as these areas were subject to different regulations under EU

Council of the EU, *Proposal for a draft Council Decision on the Establishment, Operation and Use of the Second Generation Schengen Information System (SIS II) - Redrafted proposal*, Brussels, 5710/06, 27 January 2006.

³⁴ The central infrastructure is located in Strasbourg (France) with a back-up central station in Sankt Johann im Pongau (Austria).

³⁵ See the Commission Implementing Decision 2013/115/EU of 26 February 2013 on the Sirene Manual and other implementing measures for the second generation Schengen Information System (SIS II) (notified under document C(2013) 1043), *OJ L* 71, 14.3.2013, pp. 1-36, replaced by the Commission Implementing Decision (EU) 2017/1528 of 31 August 2017 replacing the Annex to Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) (notified under document C(2017) 5893) *C/2017/5893, OJ L* 231, 7.9.2017, pp. 6-51.

³⁶ See the Council of the EU, *Options for the establishment of the legal basis for the provisions of the Schengen acquis relating the Schengen Information System*, 11561/98, Brussels, 26 October 1998, and the Council Decision 1999/307/EC of 1 May 1999 laying down the detailed arrangements for the integration of the Schengen Secretariat into the General Secretariat of the Council, *OJ L* 119, 7.5.1999, pp. 49-52.

³⁷ See Article 5(2) Protocol No 2, that establishes that the provisions of the Treaties would be applicable also if the Council would have not taken yet the decision for integrating the Schengen *acquis* in the Amsterdam Treaty.

primary Law, at least until PJCCM policies were communitarised in 2007 – currently as Title V of the TFEU.

Originally, the SIS issued alerts on persons, objects, and vehicles³⁸. Alerts on persons concerned: persons wanted for arrest for extradition purposes; third country nationals for whom an alert was issued for the purposes of refusing their entry; missing persons or persons who, for their own protection, or in order to prevent threats, temporarily needed to be placed under police protection; data on witnesses, persons summoned to appear before the judicial authorities in connection with criminal proceedings, and persons for the purposes of discreet surveillance or of specific checks. In addition, alerts on vehicles could be inserted for the purposes of discreet surveillance or for specific checks. Finally, the alerts on objects included: different categories of vehicles, firearms, and blank official documents; data for the purposes of seizure or use as evidence in criminal proceedings; stolen, misappropriated or lost identity papers, and banknotes.

The SIS did not contain any biometrics but only alphanumeric data³⁹ since it was based ‘[...] on the situation in the late eighties, when technology was not far enough advanced to allow the handling of any kind of digital images or biometric data on a permanent basis’⁴⁰. As Prof. Brouwer highlights, the Convention implementing the Schengen Agreement inserted strict rules on data protection⁴¹ that Member States should have complemented within their internal law⁴². Furthermore, additional rules were established to: coordinate the Member States in the issuing of new alerts for the purpose of consistency⁴³; guarantee the rights to access the data entered into SIS⁴⁴, including the right to a remedy⁴⁵, and to set up a new apparatus of independent authorities responsible for the lawful processing of data. According to the Council, it would have been up to the Member States to look ensure the security of the data processed in the SIS⁴⁶. In general terms, norms on data security should have included an analysis of the risks of the

³⁸ See Articles 93 to 100 of the Convention implementing Schengen Agreement.

³⁹ According to Article 94(3) of the Convention implementing the Schengen Agreement: surname and forenames, any aliases possibly entered separately; any specific objective physical characteristics not subject to change; first letter of second forename; date and place of birth; sex; nationality; whether the persons concerned are armed; whether the persons concerned are violent; reason for the alert, and action to be taken.

⁴⁰ See the Council of the EU, *Development of the Schengen Information System II and possible synergies with a future Visa Information System (VIS)*, 16106/03, Brussels, 15 December 2003, p. 15.

⁴¹ See Articles 102-118 of the Convention implementing the Schengen Agreement, and Jos Dumortier, “The Protection of Personal data in the Schengen Convention”, *International Review of Law Computers and Technology*, Vol. 11, No. 1, 1997, pp. 93-106.

⁴² See Article 104(1) of the Convention implementing the Schengen Agreement.

⁴³ See Articles 106 and 107 of the Convention implementing the Schengen Agreement.

⁴⁴ See Articles 109 and 110 of the Convention implementing the Schengen Agreement.

⁴⁵ See Article 111 of the Convention implementing the Schengen Agreement.

⁴⁶ See Article 118 of the Convention implementing the Schengen Agreement.

processing with regard to the principles of confidentiality, integrity, and availability⁴⁷. One of the basic principles developed in this field was the prohibition of sharing data with outsiders ‘[...] because it causes unreasonable difficulties to an individual and may result in damage claims. It is important that the authorities operate in such a way that the interests of the whole society, public administration and private citizens are secured in all circumstances’⁴⁸.

National supervisory authorities⁴⁹ were in charge of the supervision of the data files of the national section of the SIS and of checking that the processing and use of any data entered did not violate the rights of the data subject. A Joint Supervisory Authority was set up, it was made up of two representatives from each contracting party responsible for the technical support of the SIS. Each contracting party was liable to supply the alerts issued before the data subjects⁵⁰. In this sense, contracting parties were asked to adhere to Convention No 108⁵¹ and to follow the Recommendation of 17 September 1987 of the Committee of Ministers of the Council of Europe regulating the use of personal data within law enforcement⁵².

Access to the system was reserved to border guards and police and customs checks⁵³; yet, Member States should have regulated the access of other administrative authorities such as visa authorities, and immigration authorities that were competent for the issuing of residence permits under their own national law⁵⁴. The limited number of authorities granted access to the SIS and, specifically, the large number of criminal alerts issued confirm that the SIS was originally conceived as a police cooperation tool that, together with the Europol Convention of 1 July 1999, sped up the process of integration of the EU policies on criminal domains⁵⁵. Nevertheless, the possibility that access to the SIS alerts could be enlarged to include other types of

⁴⁷ See also the Council of the EU, *Recommended guidelines for data security in connection with Schengen Information System*, 11148/1/02, Brussels, 18 October 2002.

⁴⁸ See the Council of the EU, *Data security policy of the Schengen Information System*, 12085/99, Brussels, 15 November 1999, p. 1.

⁴⁹ See Articles 114 and 115 of the Convention implementing the Schengen Agreement.

⁵⁰ See Article 116 of the Convention implementing the Schengen Agreement.

⁵¹ See the Council of the EU, 12085/99, Brussels, 15 November 1999, p. 1.

⁵² See the Recommendation of the Committee of Ministers of the Council of Europe No. R (87) 15 regulating *the use of personal data in the police sector*, Strasbourg, 17 September 1987.

⁵³ See Article 101(1) of the Convention implementing the Schengen Agreement and the list of national authorities with direct access to SIS in, among others, the Council of the EU, *List of competent authorities which are authorised to search directly the data contained in the Schengen Information System pursuant to Article 101(4) of the Schengen Convention*, 6265/03, Brussels, 14 April 2003.

⁵⁴ See Article 101(2) of the Convention implementing the Schengen Agreement and the German request to grant access to the Bundesamt für die Anerkennung Ausländischer Flüchtlinge (BAFI – Federal Office for the Recognition of Foreign Refugees) in Council of the EU, *List of authorities allowed direct access to data stored in the Schengen Information System*, 10495/99, Brussels, 29 July 1999.

⁵⁵ See the Council Act of 26 July 1995 drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention), *OJ C* 316, 27.11.1995, p. 1-32.

authorities, as presented by the German delegation⁵⁶, suggested that this system could have potentially become a multifunctional source of information.

2.1.2. Paving the way toward the second generation of the SIS

The discussions around the establishment of the second generation of the SIS date back to 1996, though its upgrade only became indispensable in 2004 in the light of its large-scale increase in size. The political deadline for the technical development of the SIS was established as 31 December 2006 under the implementation powers of the European Commission⁵⁷. However, delays encountered during the preparation phase of the SIS II project led to an extension of the European Commission's mandate until 31 December 2008⁵⁸. Meanwhile, and in order not to excessively delay the implementation of the SIS II in new Member States, the SIS was upgraded into SISone4all⁵⁹.

The interpillar structure continued to divide the SIS into two separated areas and the Council and the European Commission took the lead of one proposal each⁶⁰. Article 66 of the 1997 TEC was the key legal basis to develop SIS II under Council Regulation (EC) No 2424/2001, while the Council Decision 2001/886/JHA was underpinned by Article 30(1)(a) and (b), Article 31(a) and (b) and Article 34(2)(c) 1997 TEU. This decision followed the CJEU's jurisprudence and the Council Legal Service's opinion that affirmed that an EU act adopted under the third-pillar structure would in no way be attributed to the Community powers⁶¹. During the preparation of

⁵⁶ See the Council of the EU, *Statement by Federal Minister Schily at the informal Council in Marseilles on 28 and 29 July 2000 on the development of police cooperation and the Schengen Information System*, 10959/00, Brussels, 31 August 2000.

⁵⁷ See Article 7 of the Council Regulation (EC) No 2424/2001 of 6 December 2001 on the development of the second generation Schengen Information System (SIS II), *OJ L* 328, 13.12.2001, pp. 4-6, and the Council Decision 2001/886/JHA of 6 December 2001 on the development of the second generation Schengen Information System (SIS II), *OJ L* 328, 13.12.2001, pp. 1-3.

⁵⁸ See the Council Regulation (EC) No 1988/2006 of 21 December 2006 amending Regulation (EC) No 2424/2001 on the development of the second generation Schengen Information System (SIS II), *OJ L* 411, 30.12.2006, pp. 1-5, and the Council Decision 2006/1007/JHA of 21 December 2006 amending Decision 2001/886/JHA on the development of the second generation Schengen Information System (SIS II), *OJ L* 411, 30.12.2006, pp. 78-81.

⁵⁹ See the Portuguese study on SISone4all in Council of the EU, *Feasibility study SIS one 4all -Schengen Information System*, 13540/06, Brussels, 12 October 2006.

⁶⁰ In accordance with the Protocol integrating the Schengen acquis into the framework of the European Union, *OJ C* 340, 10.11.1997, p. 93.

⁶¹ See the C-170/96, *Commission v Council*, 20 May 2008, EU:C:2008:288, para. 16:

‘It is therefore the task of the Court to ensure that acts which, according to the Council, fall within the scope of Article K.3(2) of the Treaty on European Union, do not encroach upon the powers conferred by the EC Treaty on the Community. It follows that the Court has jurisdiction to review the content of the Act in the light of Article 100c of the EC Treaty in order to ascertain whether the Act affects the powers of the Community under that provision and to annul the Act if it appears that it should have been based on Article 100c of the EC Treaty’.

and, on this subject, Álvaro Oliveira, “Case C-170/96, *Commission of the European Communities v. Council of the European Union*, judgment of 12 May 1998, [1998] ECR I-2763”, *Common Market Law Review*, Vol. 36, No. 1, 1999, pp. 149-155. The Legal Service Opinion is available in Council of the EU, *Opinion of the Legal Service*,

the strategic plan for the creation of the SIS II, the possibility of establishing it on the basis of a community act – a first-pillar measure – and a separate EU act – a third-pillar measure – was justified with the following reasoning: while a Community databank act should have been adopted for the input operations and the consultation of data performed by border control authorities at the EU's external borders, an EU act could have been adopted in the light of the pre-emption principle. Indeed, at that time, the European Community had not yet exercised its competences on the crossing of internal and external borders, or on immigration – see Articles 62 and 63 of the 1997 TEC, respectively – as a result, Member States fully retained their sovereign competences that could have been exercised under the intergovernmental framework of EU Law. This subdivision, in the end, was also indispensable in allocating the relevant expenditures from European Community funds. However, Member States' delegations preferred to avoid any binding decision on the choice of the correct legal basis in the light of the future development of the Schengen *acquis* individual provisions. Therefore, they suggested the elimination of any reference to the SIS objectives to flatten the first and third pillar sections⁶². As a consequence, a general reference to Article 66 of the 1997 TEC, as far as the proposed Schengen Regulation was concerned, was found to be preferable⁶³.

This position was not undertaken by the European Commission that, from that moment on, defended the “double nature” of the SIS and the idea that two legislative and parallel proposals should have been presented as a cross-pillar text was not feasible⁶⁴.

a) Spanish initiative: using the SIS to fight terrorism

While the negotiations on the development of the SIS II package were still ongoing, the Spanish delegation presented a new initiative designed to shape the SIS for the purposes of combating terrorism by virtue of the common integrated security strategy agreed after the attack on the World Trade Centre in 2001⁶⁵.

Draft EY Framework Decision on the protection of the environment through criminal law – Compliance with Community powers (Article 47 of the TEU), 6793/01, Brussels, 8 March 2001.

⁶² See the Council of the EU, *Draft Council Regulation and draft Council Decision on the development of the second generation Schengen Information System (SIS II)*, 11998/01, Brussels, 19 September 2001, p. 3.

⁶³ *Ibid.* recital (5).

⁶⁴ See the Council of the EU, 5472/02, Brussels, 29 January 2002, p. 14.

⁶⁵ See the Council of the EU, *Improving the use of the Schengen Information System and the Schengen Convention to combat terrorism*, 13920/01, Brussels, 13 November 2001. However, works on the new generation of the SIS had already started – see, among others, the Council of the EU, *Draft Council Regulation and draft Council Decision on the development of the second generation Schengen Information System (SIS II)*, 13531/01, Brussels, 6 November 2001.

Following this initiative, two regulations were adopted: Council Regulation (EC) No 871/2004 for the first-pillar alerts⁶⁶, and Council Decision 2005/211/JHA for those under the third-pillar⁶⁷. These regulations required amending the Convention implementing the Schengen Agreement in order to: expand the number of authorities with access to data entered in the SIS by including the judicial branches, Europol and Eurojust⁶⁸. A second amendment aimed at allowing authorities responsible for examining visa applications and issuing visas, as well as authorities responsible for issuing residence permits and for the administration of immigration legislation, to access certain additional information entered into the SIS which might be relevant to the performance of their duties⁶⁹, and specifically in regard to stolen, misappropriated or lost blank official documents and identity papers. A third amendment aimed at clarifying the rules on the recording of personal data transmissions⁷⁰, while a fourth aimed at enacting provisions with respect to the existence and functioning of the SIRENE offices of the Member States⁷¹.

It is interesting to note that while Council Decision 2005/211/JHA was underpinned by Article 30(1)(a) and (b), Article 31(a) and (b), and Article 34(2)(c) of the 1997 TEU, without major issues, Council Regulation (EC) No 871/2004 was initially proposed on the basis of Articles 62, 63, and 66 of the 1997 TEC, but was eventually underpinned by Article 66 of the TEC alone. This choice came from the analysis of the content and purpose of the Regulation

⁶⁶ See the Council Regulation (EC) No 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, *OJ L* 162, 30.4.2004, pp. 29-31. It shall be noted that the Council Regulation was adopted at the sunset of the Council prerogative in adopting measures under Article 67 of the 2002 TEC. Indeed, as for the 1 May 2005, the transitional period established for, among others, the measures adopted under Article 66 of the 2002 TEC would have come to an end and the Council could have not adopted the acts – see the Council of the EU, *Draft Council Regulation concerning the introduction of some new functions for the Schengen Information System, including the fight against terrorism*, 6874/04, Brussels, 27 February 2007. Nevertheless, this premature adoption should have not affected the simultaneous implementation of the two legislative measures, so that the Council was empowered to adopt *ad hoc* decisions to give its approval for each specific provision.

⁶⁷ See the Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, *OJ L* 68, 15.3.2005, pp. 44-48.

⁶⁸ See Articles 101a and 101b of the Council Regulation (EC) No 871/2004 and the Council Decision 2005/211/JHA respectively. See also the document Council of the EU, *Access by EUROPOL to the Schengen Information System (SIS)*, 5970/02, Brussels, 8 February 2002, and the contrary opinion of Austria to the access of the Agency is available in Council of the EU, *Initiative by the Kingdom of Spain with a view to adopting a Council Regulation concerning the introduction of some new functions for the Schengen Information System, in particular in the fight against terrorism*, 13036/02, Brussels, 14 October 2002. The favorable opinion of Eurojust is expressed in Council of the EU, *Schengen Information System applications for EUROJUST*, 13389/02, Brussels, 22 October 2002.

⁶⁹ See Article 1(2) and (3) of the Council Regulation (EC) No 871/2004 and of the Council Decision 2005/211/JHA respectively. In reality, this possibility had been promoted by Germany since the beginning of the '90s, see the Council of the EU, *Meeting Document of the Council (Justice, Home Affairs and Civil Protection)*, SN 4038/01, Brussels, 27 and 28 September 2001.

⁷⁰ See Article 1(4) of the Council Regulation (EC) No 871/2004 and Council Decision 2005/211/JHA.

⁷¹ See Article 1(x)(5) and (5a) of the Council Regulation (EC) No 871/2004 and of the Council Decision 2005/211/JHA respectively.

made by the Council Legal Service⁷² under the premise that the two instruments could not be merged in light of Article 47 TEU⁷³. The Council Legal Service highlighted that:

‘When the visa authorities and the immigration authorities responsible for administering legislation on third-country nationals carry out their duties, it cannot be said that this constitutes "common action in the fields of police and judicial cooperation in criminal matters" or that they are authorities responsible for "preventing and combating crime" within the meaning of Article 29 TEU’⁷⁴.

It also clarified that the purposes for which the data was entered were not relevant to determining the legal basis and that what should have been relevant were the purposes for which the authorities sought to be granted access to the data. The amendment proposed that the Convention implementing the Schengen Agreement pursued a community objective and, as such, should have been adapted under Title IV of the 1997 TEC.

Having said that, the Council Legal Service was asked whether Article 66 of the 1997 TEC *per se* may have been sufficiently defined as the sole legal basis, without reference to any other EU policies – namely Articles 62 and 63 of the 1997 TEC. At that time, the Council Legal Service underlined that, up until that point, Article 66 of the 1997 TEC had been used for the adoption of Council Regulation (EC) No 2424/2001 on the development of the second-generation SIS and for Council Decision 2002/463/EC that adopted the so-called ARGO programme⁷⁵. By looking at the community proposal, the Council Legal Service affirmed that:

‘Since the TEC-related aspects of the SIS involve cooperation between the relevant departments of the administrations of the Member States responsible for issuing visas and residence permits, for examining visa applications, and for administering immigration legislation, and since the exchange of further information by the Sirene offices assists in that end, the [Council Legal Service] considers that Article 66 TEC is the appropriate legal basis, as it allows for Community measures to ensure such cooperation. Furthermore, it considers that it is not necessary for Articles 62 and 63 TEC to be cited as the legal basis. The amendments in question only concern access to and the operation of the SIS itself and the Sirene offices; they do not concern substantive policy measures relating to the absence of controls when crossing internal borders, the crossing of external borders, or the freedom

⁷² In its opinion, the Council Legal Service recalled *Opinion 2/00*.

⁷³ Council of the EU, 6793/01, Brussels, 8 March 2001:

‘Subject to the provisions amending the Treaty establishing the European Economic Community with a view to establishing the European Community, the Treaty establishing the European Coal and Steel Community and the Treaty establishing the European Atomic Energy Community, and to these final provisions, nothing in this Treaty shall affect the Treaties establishing the European Communities or the subsequent Treaties and Acts modifying or supplementing them’.

In the Council Legal Service’s Opinion of 5 March 2001 it was stated that according to Article 47 TEU, if an area fell within the sphere of competence of the Community, it would not be legally possible to adopt common rules in that area by means of an instrument under Title VI of the TEU – see also the Opinion of Advocate General Fennelly, C-170/96, *Commission v Council*, 12 May 1998, EU:C:1998:219, paras. 8 and 9.

⁷⁴ See the Council of the EU, *Initiative of the Kingdom of Spain with a view to the adoption of a Council Regulation concerning the introduction of some new functions for the Schengen Information System* [in particular in the fight against terrorism] (document 9407/2/02). *Initiative of the Kingdom of Spain with a view to the adoption of a Council Decision concerning the introduction of some new functions for the Schengen Information System* [in particular in the fight against terrorism] (document 9408/2/02), 13713/02, Brussels, 5 November 2002, p. 6.

⁷⁵ Council Decision 2002/463/EC of 13 June 2002 adopting an action programme for administrative cooperation in the fields of external borders, visas, asylum and immigration (ARGO programme), OJ L 161, 19.6.2002, p. 11.

for third-country nationals to travel within the territory of the Member States. They do not concern substantive immigration policy measures; nor do they seek to regulate conditions of entry and residence of third-country nationals. Therefore, the [Council Legal Service] would recommend the deletion of the reference to Articles 62 and 63 TEC in the preamble of the draft Regulation⁷⁶.

As a result, the legal basis for the administrative cooperation was presented, in a manner of speaking, as a “neutral” one since the newly adopted measure was confined to the preparation, development, and operational management of the SIS II. In fact, this choice was questionable as the SIS should have been based upon substantial legal bases conferring on the EU specific competences. It seems obvious to state that any reform of a system went beyond the mere setting up and ensuring that technically functioned of the system, and it is worth being clear and stating that renovation of the SIS clearly stemmed from specific political choices undertaken after 11-S. However, it is worthy to note that the technological layer was camouflaging those choices, so that the content and purposes of the legislative measure seemed to be politically void. Furthermore, by stressing its preference toward Article 66 of the 1997 TEC, instead of Articles 62 and 63 of the 1997 TEC, the Council Legal Service was opting for a legal basis that still carried the burden of the intergovernmental framework, where the Council of the EU should have voted by qualified majority after merely consulting the European Parliament.

Finally, it is interesting to note that Council Decision 2005/211/JHA and Council Regulation (EC) No 871/2004 did not only grant access to administrative data to law enforcement authorities and EU bodies, but also to administrative authorities gaining access to categories of data that, in principle, were registered in the system for EU criminal law purposes. As a consequence, the blurring of the lines between the provisions of both the TEU and the TEC was promoted on a double track: the criminal and freedom sections overlapped with one another confusing its purpose.

b) The development of the second generation of the SIS

The development of the SIS II aimed to:

- establish its compatibility with other existing – and future – databases⁷⁷;
- be more flexible so as to enable new Member States and EU agencies to join it;
- store new types of data, including biometrics⁷⁸, and
- link different correlated alerts.

⁷⁶ Council of the EU, 13713/02, Brussels, 5 November 2002.

⁷⁷ See the Council of the EU, 16106/03, Brussels, 15 December 2003, p. 5.

⁷⁸ A summary of the new category of data entered in the SIS II is available here Council of the EU, *Proposal for a Council Regulation on migration from the Schengen Information System (SIS I+) to the second generation Schengen Information System (SIS II) (recast) – New data categories and functionalities in SIS II*, 13057/12, Brussels, 31 July 2012.

As a result, from an architectural point of view, the SIS II maintained its peculiar structure made of a N-SIS and a C-SIS so that the N-SIS could store a complete or partial copy of the SIS II database.

In June 2005, the European Commission presented a new SIS II package to develop the system on the basis of three proposals:

- one for the development of the SIS II under the criminal law framework⁷⁹;
- another for use by the SIS II administrative authorities⁸⁰ and, finally,
- a third one to establish access by national authorities responsible for the registration of vehicles to specific SIS II alerts⁸¹.

Starting with the last proposal, access to the SIS II was sought by national vehicle registration authorities in order to make them aware of alerts on stolen, misappropriated or lost vehicles. Since this access was not granted by the Convention implementing the Schengen Agreement, it was uncertain whether the amendments should have been applied through the intergovernmental framework of the Convention implementing the Schengen Agreement or under Community Law. The Council Legal Service affirmed that the Council was entitled to adopt such measure since:

‘[...] the Community, with Article 9 of the Directive, has begun to exercise its powers, but is far from having exhausted them. Action by Member States is therefore possible provided that it complies with the Treaties, and the principle of cooperation as laid down in Article 10 of the TEC and is compatible with the measures already adopted by Community bodies’⁸².

As for the adequate law-making procedure, the Council Legal Service admitted that the choice between a framework decision and a convention under Article 30 of the 2002 TEU was a political one, yet the latter was preferable as it would have involved the scrutiny of the national parliaments according to the principle of subsidiarity. The services in charge of issuing vehicle registration certificates were finally granted access to the SIS II under Regulation (EC) No 1986/2006⁸³, though its adoption left unresolved the German dissatisfaction regarding the

⁷⁹ See the Council of the EU, *Proposal for a Council Decision on the establishment, operation and use of the second generation Schengen information system (SIS II)*, 9942/05, Brussels, 9 June 2005.

⁸⁰ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen information system (SIS II)*, 9943/05, Brussels, 9 June 2005.

⁸¹ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates*, 9944/05, Brussels, 9 June 2005.

⁸² See the Council of the EU, *Access to the Schengen Information System (SIS) for vehicle registration authorities*, 9731/99, Brussels, 12 July 1999, p. 5.

⁸³ Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates, *OJ L* 381, 28.12.2006, pp. 1-3.

choice of the correct legal basis⁸⁴. The chosen legal basis was Article 71(1)(d) of the 2002 TEC on the adoption of measures on distinctive features of transport instead of Articles 30(1)(a) and (b) of the 2002 TEU on PJCCM. This “transportation” of the legal basis from the third pillar to the first was not sufficiently justified by the European Commission according to the EDPS as the rationale behind granting access to the SIS II should have been justified in the light of the prevention of, and fight against, the trafficking of stolen vehicles⁸⁵.

As for the SIS II alerts, a council decision should have been adopted in order to embrace the third-pillar approach⁸⁶. The Council Decision 2007/533/JHA wanted to insert a new category of alerts in relation to the adopted European Arrest Warrant Framework Decision⁸⁷ and to improve the available information on persons whose identity could have been abused⁸⁸. It is interesting to point out Prof. Peers’ opinion, who underlines how the SIS II Council Decision 2007/533/JHA on criminal law alerts was incorrectly adopted on the basis of Articles 30(1)(a) and (b)⁸⁹, 31(1)(a) and (b),⁹⁰ and 34(2)(c) of the 2002 TEU⁹¹. According to the author, Article

⁸⁴ See the Council of the EU, *Proposal for a Council common position on: Draft Regulation of the European Parliament and of the Council amending the provisions of the Convention implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at common borders as regards access to the Schengen Information System by the authorities and services in the Member States responsible for issuing registration certificates for vehicles*, 13824/04, Brussels, 22 October 2004.

⁸⁵ See the Council of the EU, *Opinion of the European Data Protection Supervisor on the legislative proposals concerning the Second Generation Schengen Information System (SIS II)*, 14091/05, Brussels, 14 November 2005, p. 16.

⁸⁶ Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), *OJ L* 205, 7.8.2007, pp. 63-84.

⁸⁷ See the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision, *OJ L* 190, 18.7.2002, pp. 1-20. A specific proceeding is foreseen in case a judicial authority has refused to execute a European Arrest Warrant as well as when it is obvious that the execution of the European Arrest Warrant will be refused. In this case the SIRENE Bureau should add a “flag” to the alert according to Article 25 of the Council Decision 2007/533/JHA.

⁸⁸ Also, in the air, it seems that secret services too were granted access to the SIS II, though from the sources founded it is not understandable how or where. In this regard, the European Parliament’s complained on the introduction of this new element just forty-eight hours before the vote of the LIBE Committee on the draft report – see the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen information system (SIS II) – Outcome of the European Parliament’s first reading (Strasbourg, 23 to 26 October 2006)*, 14296/06, Brussels, 27 October 2006.

⁸⁹ See Article 30(1)(a) of the 2002 TEU:

‘Common action in the field of police cooperation shall include: (a) operational cooperation between the competent authorities, including the police, customs and other specialised law enforcement services of the Member States in relation to the prevention, detection and investigation of criminal offences; (b) the collection, storage, processing, analysis and exchange of relevant information, including information held by law enforcement services on reports on suspicious financial transactions, in particular through Europol, subject to appropriate provisions on the protection of personal data [...]’.

⁹⁰ See Article 30(1)(b) of the 2002 TEU: ‘Common action on judicial cooperation in criminal matters shall include: [...] (b) facilitating extradition between Member States; [...]’.

⁹¹ See Article 34(2)(c) of the 2002 TEU:

‘In the areas referred to in this title, Member States shall inform and consult one another within the Council with a view to coordinating their action. To that end, they shall establish collaboration between the relevant departments of their administrations. [...] (c) adopt decisions for any other purpose consistent with the objectives of this title, excluding any approximation of the laws and regulations of the Member States. These

30(1)(a) of the 2002 TEU on operational cooperation among competent authorities, including the police, customs, and other specialised law enforcement services, should have been excluded from the legal framework since the operational activities developed therein were far less important than the flow of information generated through the system⁹². However, this choice was consistent with the legal framework of Regulation (EC) No 1987/2006, where Article 66 of the TEC was still perceived as the relevant legal basis and, even more importantly, it pointed out which authorities were granted access to the system.

The SIS II Council Regulation on refusal of entry alerts was adopted on the basis of Articles 62(2)(a) and 63(3)(b) of the 2002 TEC to cover EU policies on checks on persons at its external borders and the prevention of, and fight against, irregular migration⁹³. In addition, Article 66 of the 2002 TEC was inserted to underpin the EU competence in the practical cooperation among administrations, and between them and the European Commission. However, in its proposal, the European Commission only contemplated Articles 66 and 62(2)(a) of the 2002 TEC on the assumption that:

‘The legal basis of Article 66 can also cover provisions on what authorities have access to the SIS II; thus, the proposal allows for the access of the authorities responsible for external borders, visas, asylum and immigration’⁹⁴.

Once again, the Council Legal Service expressed its opinion and, even if its analysis is not accessible to the public, it seems reasonable that it urged the European Commission to insert references to other substantial legal bases. This may be inferred by the readable incipit, which claims that:

‘[...] a distinction can be made between the provisions concerning the establishment and functioning of the SIS as a tool for cooperation between the relevant departments of the administrations of the Member States, including the establishment of procedures and rules on data protection and liability, on the one hand, and the provisions seeking to

decisions shall be binding and shall not entail direct effect; the Council, acting by a qualified majority, shall adopt measures necessary to implement those decisions at the level of the Union [...]’.

⁹² Steve Peers, *EU Justice and Home Affairs Law. Volume II: EU Criminal Law, Policing, and Civil Law*, Oxford, Oxford EU Library, 2016, p. 272:

‘[...] many of the Council’s decisions regarding legal bases could be questioned: for instance, the Decision establishing SIS II, which was in part adopted on the legal base of the previous Article 30(1)(a) TEU, addressed operational police cooperation marginally, to the extent that it set out rules for action following policing alerts; but essentially it concerned only the collection of information, and should have had only Article 30(1)(b) TEU (now Article 87(2)(a) TFEU) as a legal base’.

⁹³ Which required the adoption of the co-decision procedure – see the Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006, on the establishment, operation and use of the second generation Schengen Information System (SIS II), *OJ L* 381/4, 28.12.2006.

⁹⁴ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II) - Legal Base*, 11380/05, Brussels, 20 July 2005.

harmonize the standards for issuing alerts for the purpose of refusing entry, on the other hand⁹⁵.

In any case, the delegations felt it necessary to introduce harmonised rules for accessing refusal of entry alerts given the lack of a common regulation on the return of third country nationals⁹⁶. Indeed, it was only when the Return Directive⁹⁷ entered into force that the SIS II alerts on entry-bans were directly linked to the EU policy on the prevention of, and fight against, irregular migrants. From the time being, Regulation (EC) No 1987/2006 did not oblige Member States to insert data regarding individuals subject to an expulsion, refusal of entry or transfer measure accompanied by a ban on entry or residence following a case of non-compliance with a Member State's internal entry or residence rules⁹⁸. This concession shows that the SIS II was still conceived as a tool for combating cross-border crime rather than as a mechanism to address the administrative irregularities of third-country nationals.

As for its content, Council Regulation (EC) No 189/2008 aimed at harmonising the divergent practices of the Member States when inserting refusal of entry alerts⁹⁹ while providing additional access rights to asylum and immigration authorities. The differing ways in which Member States made use of the refusal of entry alert under Article 96 of the Convention implementing the Schengen Agreement was critical and the Schengen Joint Supervisory Authority called for further harmonisation. The new framework also sought to clarify which authorities had access to the system, why alerts were issued and, finally, the establishment of a five-year retention period.

The new legal framework set forth under the Council Decision and the Council Regulation introduced crucial changes to regulate the SIS II. As the EDPS underlined, the SIS II had a

⁹⁵ *Ibidem*. See also the scrutiny reservation of the Commission on this legal basis in Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II)*, 5709/3/06 REV 3, Brussels, 24 April 2006.

⁹⁶ See the Belgian position in the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II) – Redrafted proposal*, 5709/1/06 TEV 1 ADD 6, Brussels, 4 April 2006.

⁹⁷ Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals, *OJ L* 348, 24.12.2008, pp. 98-107 (Return Directive hereinafter). Confront Teresa Fajardo del Castillo, “La directiva sobre el retorno de los inmigrantes en situación irregular”, *Revista de Derecho Comunitario Europeo*, No. 33, 2009, pp. 453-499.

⁹⁸ See Article 24(3) of the Regulation (EC) No 1987/2006 and Pieter Boeles, Maarten den Heijer, Gerrie Lodder and Kees Wouters, *European Migration Law*, Cambridge, Intersentia, 2014, p. 402. On the contrary, the Regulation (EC) No 1987/2006 obliged Member States to insert data only in cases where third-country nationals would have posed a threat to the security of EU citizens, according to Article 23(1) and Article 26. It should be noted in this regard that the Spanish translation of Article 24 is liable to cause confusion by establishing in the three situations that the Member States “may” enter the data of third-country nationals. However, from a comparison with the legislative texts in English, French and Italian, we can infer the need to distinguish between the duty and the power to insert these data in the SIS II.

⁹⁹ See Articles 15 and 16 of the Council Regulation (EC) No 1987/2006.

broader scope than the SIS under the Convention implementing the Schengen Agreement, and '[t]he transformation of an intergovernmental structure into European law instruments brings several positive consequences: the legal value of the rules governing SIS II will be clarified, the Court of Justice will have competence for the interpretation of the first pillar legal instrument), the European Parliament will be at least partly involved (albeit a little late in the process) [...] Moreover, on substance, the proposals contain a significant part devoted to data protection, some of which being welcome improvements compared to the current situation'¹⁰⁰. On the contrary, the transition from the intergovernmental framework to the interinstitutional one was not immediately palatable to the Member States¹⁰¹.

First of all, the SIS II legislation enabled the insertion of biometric data – photographs and fingerprints – to confirm the individuals' identity through verification, as well as being used to detect the use of false identities or documents, and to discern namesakes. As for the use of biometric data, the EDPS called for major safeguards because of the sensitivity of the data and the lack of a relevant common regulation regarding it. The EDPS complained of the lack of an explanatory memorandum and of an impact assessment that would have helped assess the proportionality of the impact of the European Commission's proposal on the individuals' fundamental rights. It emphasised the necessity to safeguard the enrolment procedure for the Failure to Enrol (FTE) and Failure to Capture (FTC) Rates¹⁰² as well as the level of accuracy of the data and recommended the implementation of a fall back procedure. The European Parliament, for its part, remarked that before fingerprints became the main search criteria, a decision had to be taken according to the co-decision procedure – i.e., their use had to be scrutinised. Meanwhile, the European Commission should have reported to the European Parliament on the availability and reliability of the technology used in the biometric comparisons.

From that moment on, alerts in the SIS II could have been interlinked under the association of national rules. The EDPS then underlined that linking data is usually an investigative tool that represents a new form of processing personal data and, as such, the purpose of processing

¹⁰⁰ See the Council of the EU, 14091/05, Brussels, 14 November 2005, p. 3.

¹⁰¹ See the comments of the delegations in the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II)*, 14498/05, Brussels, 16 November 2005, and especially the scrutiny reservations made by France and Spain that wanted the Commission to withdraw the proposals and opt for an amendment of the Convention implementing the Schengen Agreement.

¹⁰² FTE is the 'failure to create and store a biometric enrolment data record for an eligible biometric capture subject, in accordance with a biometric enrolment policy' and FTC is 'failure of the biometric capture process to produce a captured biometric sample of the biometric characteristic of interest' according to the ISO/IEC 2382-37:2017, Information technology — Vocabulary — Part 37: Biometrics, para. 3.9.6 and para. 3.9.5.

should be clarified¹⁰³. Each link should have had a clear, defined relationship with the others, and in full compliance with the proportionality principle. In this sense, the authorities with no right to access certain categories of data could not have access to the links between the data, but should not have even be aware of their existence.

The SIS II regulation integrated the new European Community's framework on the protection of personal data as adopted by the DPD and the DPREC. In fact, the lack of any measure on the protection of personal data processed under the third-pillar activity should have been filled-in by reference to Council of Europe's Convention 108 that had already been ratified by all the Member States¹⁰⁴. According to the co-legislators, the rationale behind the insertion of data protection norms in the legislative measure regulating a system should have been interpreted in the light of the *lex specialis derogat generali* principle. As a consequence, the rules set forth in the SIS II regulation should have conformed with the general rules that remained applicable to able to fill in the legislative gaps. However, as the EDPS underlined, this legislative technique was justified at a time when the CFREU was not binding on the Member States, so that the data protection general framework should have been specified in light of its application in the AFSJ. The EDPS maintained that this choice '[...] should never lead to a watering down of the level of data protection ensured under the Directive or Convention¹⁰⁵'. Moreover, the adoption of two different legal frameworks for the first and third pillars, though justified in light of the legal bases, should have not lowered the guarantees set forth in the Convention implementing the Schengen Agreement. The EDPS highlighted that, while the DPD provided for some exceptions to the purpose limitation principle in case of important interest – national security, defiance, public security –, this was not in the spirit of the Convention implementing the Schengen Agreement, whose Article 102 established a strict interpretation of the purpose limitation principle so that any processing of data outside the scope of Articles 1 to 4 should be perceived as misuse. The EDPS suggested maintaining the wording of the Convention implementing the Schengen Agreement to limit the possibility for Member States to use the data in ways not foreseen in the SIS II texts. In any case, the EDPS pointed

¹⁰³ See also the Council of the EU, *Opinion 116/2005 on the Proposals for a Regulation of the European Parliament and of the Council (COM (2005) 236 final) and a Council Decision (COM (2005) 230 final) on the establishment, operation and use of the second generation Schengen information system (SIS II) and a Proposal for a Regulation of the European Parliament and of the Council regarding access to the second generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM (2005) 237 final)*, 14967/05, Brussels, 11 January 2006, p. 16, that states: '[...] the interlinking of alerts coming from several countries should be ruled out expressly, because it would alter the rules applying to liability for the processing of personal data and produce distorted effects in terms of supervision and control by national and central data protection authorities'.

¹⁰⁴ See Chapter I.

¹⁰⁵ See the Council of the EU, 14091/05, Brussels, 14 November 2005, p. 3.

out that: ‘The legal framework is so complex that it is very likely to engender some confusion in the practical application. It is in some cases difficult to see how *lex generalis* and *lex specialis* interact, and it would be useful to clarify this in the proposals’¹⁰⁶. The Article 29 DPWP complemented this insight analysis by remarking that the reference made in both the Council Regulation and the Council Decision to Article 13 DPD, enabling Member States to derogate or restrict data subjects’ rights in some specific cases, was constraining the Member States’ directionality by using these clauses:

‘[...] if a Community instrument such as the proposed Regulation introduces measures concerning exactly [the provisions laid down, in particular, in Article 13], that instrument could be considered as providing a harmonized approach and thus override the said discretionary powers. This means that there would be no room left to the Member States to introduce additional national measures in this sector, except where it is necessary for the purposes of concrete implementation of the Community instrument(s) in question’¹⁰⁷.

However, the provisions set forth in the proposed Council Regulation and Council Decision were not in line with the DPD’s dispositions, specifically: ‘[...] a “rewriting” of the contents of certain provisions, which are sometimes incomplete [...] gives rise to a sort of *lex specialis* or new categories of data protection provisions in the first pillar’; yet, the inconsistencies between the proposed measures and the data protection framework should have not infringed on the guarantees set forth in the latter.

The data protection legal framework carried its administrative structure into the SIS II regulation by introducing the supervision of the EDPS and the national supervisory authorities. The EDPS was empowered to monitor the European Commission’s activity while processing personal data, especially in the light of the operational management of the system; the latter should have monitored the lawful processing of data by administrators and police bodies. These authorities were called to cooperate in a joint supervisory structure that was welcomed by the EDPS as it was similar to the Article 29 DPWP in terms of organisation¹⁰⁸. Nevertheless, the EDPS noted that although the European Commission was formally given responsibility for the operational management of the system, its role was far more important. Indeed, the European Commission should have also covered the implementation and management of the system under the comitology procedure. In the EDPS’s eyes, this should have been considered as a *sui generis* position between the data processor and data controller functions as the European Commission had no access to the data:

¹⁰⁶ *Ibidem*.

¹⁰⁷ See the Council of the EU, 14967/05, Brussels, 11 January 2006, p. 11 ff.

¹⁰⁸ Article 29 DPD.

‘There is some fuzziness in the attribution of competences between Member States and the Commission. Clarity is paramount as it is not only necessary for the smooth running of the system, but also a basic requirement to ensure a comprehensive supervision of the system’¹⁰⁹.

The EDPS recommended that both the European Commission and the Member States be considered as joint controllers so as to share the responsibility of the lawful processing of data. This would have also been relevant before the exercise of data protection subjective rights, for which purpose the right to a remedy should have also been granted to third country nationals, no matter the geographical limitations¹¹⁰.

The new SIS II was innovative in that it would have enabled the transfer of data toward third countries and international organisations¹¹¹. Of particular interest is the possibility of transferring information on passports to Interpol, which should have been sealed by an international agreement subject to the consensus of the Member State’s owning of the data entered into the system¹¹². The Article 29 DPWP explicitly states that:

‘[...] the very possibility of transmitting information to those third parties – which would be a decision falling in any case within the scope of competence of the individual Member States and only apply to the data owned by them, given the system configuration – does not appear to be in line with the purposes of the system as it is currently configured’¹¹³.

The establishment of the agreement should have been backed by a European Commission adequacy evaluation on the level of protection of personal data guaranteed by Interpol’s Member States. Indeed, not only would Member States have been granted access to Interpol’s database, but Interpol’s members would be enabled to search in the SIS II through the Interpol’s channels¹¹⁴.

The EDPS complained about the different categories of access granted to the SIS II. The Article 29 DPWP classified them as a breach of the purpose limitation principle. Europol and Eurojust were granted access to the system to achieve their own purposes which, in the EDPS’s opinion, constituted a too broad definition that impeded their compliance with the data protection laws. The EDPS suggested limiting access to cases where the names of persons

¹⁰⁹ Council of the EU, 14967/05, Brussels, 11 January 2006.

¹¹⁰ See the Council of the EU, *Joint Declaration of the Commission, the Council and the European Parliament*, 17003/06 ADD 1, Brussels, 19 December 2006. All in all, the European Commission’s mandate was temporally as a new Agency would have soon undertaken the operational management of the system as we will explore in due course.

¹¹¹ Article 48 of the Council Decision 2007/533/JHA. See the Council of the EU, *Transfer of personal data to third parties: Article 48 of the Council Decision on the establishment, operation and use of the second generation Schengen Information System (SIS II)*, 14092/05, Brussels, 9 December 2005.

¹¹² See Article 55 of the Council Decision 2007/533/JHA.

¹¹³ See the Council of the EU, 14091/05, Brussels, 14 November 2005, p. 15.

¹¹⁴ See the Council of the EU, *Council’s declaration in Council Decision on the establishment, operation and use of the second generation Schengen Information System (SIS II)*, 10403/07, Brussels, 8 June 2007, p. 5.

would have already been in their files, with the specific aim of avoiding “fishing expeditions”. It also suggested avoiding the multiplication of the number of access points for security reasons. Access to data should have been justified for the purposes of the SIS II and should have been consistent with the legal bases. The compliance with those requisites should have been scrutinised by submitting a list of persons entitled to access SIS II:

‘The fact that these authorities are granted access to SIS II data can never be a ground for entering or maintaining data in the system if they are not useful for the specific alert, they are part of. New categories of data may not be added because they would benefit other information systems. For example, Article 39 of the proposed Decision provides for the introduction of alerts on data concerning the issuing authority. These data are not needed to perform an action (arrest, surveillance,...), and the only reason why they could be introduced is probably to benefit Europol or Eurojust. A clear rationale for the processing of this data should be provided’¹¹⁵.

With the SIS II, the overall retention period was extended to five years instead of the three years set forth in the Convention implementing the Schengen Agreement and a further extension was foreseen in case Member States decided that it was required. The EDPS highlighted that ‘[t]he retention period of the data may not be extended where it is not necessary for the purpose for which the data was entered’¹¹⁶. Furthermore, Member States would be authorised to retain “off-line” databases to store copies of the SIS II alerts for a period of twenty-four hours, extendable in cases of emergency.

Difficulties encountered during the testing phase seriously delayed the implementation of SIS II¹¹⁷. The extension of the European Commission mandate to enable SIS 1+ to migrate to SIS II was proposed on the basis of two regulations that were subjected to several amendments. First, Council Regulation (EC) No 1104/2008¹¹⁸ and Council Decision 2008/839/JHA¹¹⁹ were adopted for the first and third-pillar measures respectively¹²⁰. However, in 2009, the entry into force of the Treaty of Lisbon imposed the revision of the latter and a new proposal was

¹¹⁵ See the Council of the EU, 14091/05, Brussels, 14 November 2005.

¹¹⁶ *Ibidem*.

¹¹⁷ See the European Court of Auditors, *Lessons from the European Commission’s development of the second generation Schengen Information System (SIS II)*, Luxembourg, 2014.

¹¹⁸ Council Regulation (EC) No 1104/2008 of 24 October 2008 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II), *OJ L* 299, 8.11.2008, pp. 1-8.

¹¹⁹ Council Decision 2008/839/JHA of 24 October 2008 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II), *OJ L* 299, 8.11.2008, pp. 43-49.

¹²⁰ See the Council of the EU, *Opinion of the European Data Protection Supervisor on the proposal for a Council Regulation on migration from the Schengen Information System (SIS) to the second generation Schengen Information System (SIS II) (recast)*, 12530/12, Brussels, 12 July 2012.

submitted in 2010¹²¹. This gave rise to Council Regulation (EU) No 542/2010¹²². Finally, two Council Regulations were adopted in 2012: Council Regulation (EU) No 1273/2012¹²³ and Council Regulation (EU) No 1272/2012¹²⁴. It should be noted that while Council Regulation (EC) No 1104/2008 was underpinned by Article 66 of the 2002 TEC and Council Decision 2008/839/JHA by Articles 30(1)(a) and (b), 31(1)(a) and (b), and 34(2)(c) of the 2002 TEU, so as to reflect the interpillar structure existing before the Treaty of Lisbon, Council Regulation No (EU) 1273/2012 and Council Regulation (EU) No 1272/2012 were both underpinned by Article 74 TFEU; yet, the participation of the United Kingdom and Ireland and the limitations the two countries place on their membership forced a splitting of the acts¹²⁵. This change, together with the other substantial modifications inserted in the text, should have been highlighted by the European Commission according to the Article 29 DPWP that, in general terms, did not oppose them¹²⁶.

Although it might be alleged that the migration of the SIS+1 to the SIS II was a purely technical measure unrelated to any EU policy of the AFSJ, the “migration strategy” was also relevant from a data protection perspective¹²⁷. First of all, diverging from the initial proposals, the legal framework of the SIS II would have been implemented as soon as one Member State successfully migrated to the SIS II, without waiting for the others. Based on the EDPS’ evaluation, this solution was better than the previous one, as it would guarantee the simultaneous application of the new framework to all Member States while avoiding the uncomfortable situation where the new functionalities of the SIS II could be implemented by Member States still bound by the old framework – namely Title IV of the Convention implementing the Schengen Agreement. Nevertheless, the EDPS complained about the lack of consistency between the regulations and the migration plan, that should have been described in further detail so as to understand its scope, the need of a specific impact assessment, a testing

¹²¹ See the Council of the EU, *Council Regulation amending Decision 2008/839/JHA on migration from the Schengen Information System (SIS I+) to the second generation Schengen Information System (SIS II)*, 10126/10, Brussels, 2 June 2010.

¹²² Regulation (EU) No 542/2010 of 3 June 2010 amending Decision 2008/839/JHA on migration from the Schengen Information System (SIS I+) to the second generation Schengen Information System (SIS II), *OJ L* 155, 22.6.2010, pp. 23-26.

¹²³ Council Regulation (EU) No 1273/2012 of 20 December 2012 on migration from the Schengen Information System (SIS I+) to the second generation Schengen Information System (SIS II) (recast), *OJ L* 359, 29.12.2012, pp. 32-44.

¹²⁴ Council Regulation (EU) No 1272/2012 of 20 December 2012 on migration from the Schengen Information System (SIS I+) to the second generation Schengen Information System (SIS II) (recast), *OJ L* 359, 29.12.2012, pp. 21-31.

¹²⁵ On variable geometry see Chapters I and V.

¹²⁶ See the Council of the EU, *Proposal for a Council Regulation on migration from the Schengen Information System (SIS I+) to the second generation Schengen Information System (SIS II)*, 13463/12, Brussels, 7 September 2012.

¹²⁷ See the Council of the EU, 12530/12, Brussels, 12 July 2012.

phase before the beginning of the migration phase, and the requirement for the validation of the first successful test before enabling the start of the migration phase.

Second, the EDPS asked the European Commission to be more precise with regards to the data – alerts and operations’ records – that would migrate from the SIS+ to the SIS II. In this sense, the lawfulness of data processing activities should have ensured a traceability of the operations associated with the maintenance and continuation of the development of the SIS II. Any record associated with the migration activity should have not been stored for a period of over six months. The migration of data from one system to the other was considered to be a processing activity and one that carried risks that should have been assessed accordingly by the European Commission. Indeed, the migration of data implied its conversion in order to be used within the new system. In this sense, the data should have remained integrated during the period in which it was transferred into the SIS II and when the rules on the validation of the accuracy of the data would have been relaxed so as to render data and system compatible.

Finally, the EDPS noted that the completion of the testing phase that would have allowed for the start of the migration operations, or the switching to an alternative plan, was not clear and left a margin of discretion in the hands of the European Commission and the Council of the EU, a margin that raised legal uncertainty. In case of a failure in the testing, the regulation should have ensured a fall back procedure that would have allowed the Member States to temporally use the SIS+. In any case, no “real data” should have been used for testing or, in other words, the reconstruction of the data should not have been possible¹²⁸.

The SIS II could finally be set into motion on 9 April 2013 under the unanimous Decision of the Council representing Member States participating in the SIS+¹²⁹. However, considerable criticism arose from the German delegation¹³⁰ that complained about: the testing strategy used by the Commission and the consequent risks for the migration strategy; the lack of an emergency plan for the technical migration, and the non-compliance of SIS II with the four-minute timeline for the circulation of alerts as established under the legal framework¹³¹. The

¹²⁸ ‘However, once personal data may be used for testing purposes there is no additional safeguard on who can access those data and how and when such data may be used (e.g.: what kind of safeguards should eu-LISA implement when employing external contractors for performing those tests?)’ in the Opinion of the EDPS No. 07/2016 on *the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations)*, Brussels, 21.09.2016, p. 15.

¹²⁹ See Articles 71(2) of the Council Decision 2007/533/JHA and Article 55(2) of Council Regulation (EC) No. 1987/2006.

¹³⁰ See the Council of the EU, - *Council Decision fixing the date of application of Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System (SIS II) - Council Decision fixing the date of application of Regulation (EC) No 1987/2006 of the establishment, operation and use of the second generation Schengen Information System (SIS II)*, 6937/13, Brussels, 28 February 2013.

¹³¹ Article 71(3)(c) and 55(3)(c) of the Council Decision 2007/533/JHA and Regulation (EC) No 1987/2006 respectively.

lessons learned from SIS II's rolling out should have been vital when considering the implementation of new forthcoming databases including, among others, the EES¹³².

2.2. A “second” second generation of the SIS

In 2016, the European Commission presented a new report on the integration of the Automated Fingerprint Identification System (AFIS) on the SIS II¹³³, as requested by the co-legislators during the negotiations¹³⁴. The possibility of integrating the AFIS into this large-scale IT system aimed at enabling biometric searches and, as we will analyse further below, it had already been experimented with as part of the Eurodac and the VIS, yet the peculiar architecture of the SIS II delayed the implementation of the AFIS. Based on the Commission Joint Research Centre report¹³⁵, the European Commission highlighted that the technology was ready and that, despite the existence of challenges that needed to be addressed, the AFIS could have been integrated into the SIS II. As a consequence, the SIS II would have enabled biometric identification in the central database thanks to the one-to-many data comparison. The AFIS searches would not have replaced the possibility of performing a biometric verification, or a one-to-one comparison, that requires a previous search with the use of alphanumeric data – namely name and date of birth –, but it would have complemented this functionality.

From the same study, it can be inferred that the performance of the AFIS in the SIS II should have been analysed on the basis of different parameters, specifically: the quality of data entered in the system; the size of the database, the number of prints used for the search and the expected response time of the queried database, by assuming that a ten-to-ten print search would ensure the lowest error rates possible – around 0.1%. As for the quality of data, latent prints stood out as the most challenging ones. Usually found at crime or incident scenes, the enrolment phase

¹³² See the Council of the EU, *Draft Council Conclusions on the Court of Auditors' Special Report No 3/2014 "Lessons from the European Commission's development of the second generation Schengen Information System (SIS II)"*, 12285/14, Brussels, 17 September 2014.

¹³³ See the Council of the EU, *Report from the Commission to the European Parliament and the Council, The availability and readiness of technology to identify a person on the basis of fingerprints held in the second generation Schengen Information System (SIS II)*, 6720/16, Brussels, 2 March 2016.

¹³⁴ According to Article 22(c) of the SIS II Council Decision 2007/533/JHA and the SIS II Regulation (EC) No 1987/2006.

¹³⁵ See Laurent Beslay and Javier Galbally, *Fingerprint identification technology for its implementation in the Schengen Information System II (SIS-II)*, Publications Office of the European Union, EUR 27473 EN, Luxembourg, 2015. To these reports, two other studies followed: Javier Galbally Herrero, Pasquale Ferrara, Rudolf Haraksim, Apostolos Psyllos, and Laurent BESLAY, *Study on Face Identification Technology for its Implementation in the Schengen Information System*, Publications Office of the European Union, EUR 29808 EN, Luxembourg, 2019, and Alexander Angers, Dafni Maria Kagkli, Laura Oliva, Mauro Petrillo, and Barbara Raffael, *Study on DNA Profiling Technology for its Implementation in the Central Schengen Information System*, Publications Office of the European Union, EUR 29766 EN, Luxembourg, 2019.

of latent prints is not controlled with appropriate data quality checks¹³⁶. On the contrary, the Joint Research Centre suggested that the capture of biometric samples should have been performed through an electronic scanning machine – so-called “flat and rolled prints” –, preferably under the supervision of an experienced operator, as this was believed to be the most reliable procedure. As a result, the report recommended the use of latent prints for consultation purposes only.

Another parameter needed to estimate the AFIS’ performance was response time. This was a crucial element to allow fast checks at border controls, where two fingerprints, instead of ten, may be scanned. Unlike Eurodac, which performed the comparison within an hour, and the VIS that crossmatched data in less than twenty minutes, the SIS II was expected to respond in a few seconds and, as such, a biometric match should have been made in less than thirty seconds. The result was that the accuracy would have been lowered in order to privilege fast-track procedures at the borders as well as for law enforcement purposes. Ten fingerprints comparisons were thought to be necessary only in cases of necessity during second-line checks.

The operational plan presented by the European Commission laid out the implementation of the SIS II in three stages¹³⁷. First, by the end of 2019, Europol and the teams deployed by the EBCG Agency should have been granted access to the SIS II; second, by the end of 2020 all Member States should have been able to use the AFIS technology; and finally, by the end of 2021 all the provisions established in the new Regulations should have been implemented¹³⁸. In the future, AFIS is expected to be replaced by the Automated Biometric Identification System (ABIS) in order to perform identification searches not only with fingerprints, but also with photographs, other facial images and palm prints¹³⁹.

¹³⁶ To measure the fingerprint quality data the NFIQ and NFIQ-II (American National Institute for Standards and Technology (NIST) Fingerprint Image Quality) are generally used as universal model standards.

¹³⁷ See the Council of the EU, *Report from the Commission to the European Parliament and the Council on the state of play of preparations for the full implementation of the new legal bases for the Schengen Information System (SIS) in accordance with Article 66(4) of Regulation (EU) 2018/1861 and Article 79(4) of Regulation (EU) 2018/1862*, 6463/20, Brussels, 28 February 2020.

¹³⁸ At the time of our writing, few Member States have not completed the implementation of the AFIS technology – see the Report from the Commission to the European Parliament and the Council on the state of play of preparations for the full implementation of the new legal bases for the Schengen Information System (SIS) in accordance with Article 66(4) of Regulation (EU) 2018/1861 and Article 79(4) of Regulation (EU) 2018/1862, COM(2021) 336 final, Brussels, 29.6.2021. It shall be noted that the European Commission’s initial plan was even more ambitious: the AFIS should have been tested in six Member States at first, and to the other Member States by mid-2017, in order to be finally integrated into the SIS II on the 5 March 2018 – see the Council of the EU, *Information Technology (IT) measures related to border management a) Systematic checks of external borders b) Entry/Exit System (EES) c) Evolution of the Schengen Information System (SIS) d) EU Travel Information and Authorisation System (ETIAS) e) High-Level Expert Group on Information Systems and Interoperability = Progress report*, 12661/16, Brussels, 3 October 2006, p. 5.

¹³⁹ See recital (2) of Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing

In 2006, the European Commission presented the first policy evaluation report of the SIS II¹⁴⁰ with the support of eu-LISA's statistical analysis¹⁴¹. The evaluation report was accompanied by a new SIS II package that included:

- a Proposal for a Regulation from the European Parliament and of the Council on the use of the SIS for the return of third-country nationals illegally staying in a Member State¹⁴²;
- a Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation, and use of the Schengen Information System in the field of border checks¹⁴³, and
- a Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation, and use of the Schengen Information System in the field of police cooperation and judicial cooperation in criminal matters¹⁴⁴.

Although the proposals initially wanted remove the Member States' national copies of the data, the system's old architecture has been maintained. The existence of national copies was judged by the EDPS as a double-edged weapon: on one hand, it ensures the availability of the data in case of a security incident that may undermine the central database; on the other, it multiplies the copies of the data, which goes against the data minimisation principle. According

Regulation (EC) No 1987/2006 PE/35/2018/REV/1, *OJ L* 312, 7.12.2018, pp. 14-55, and recital (2) Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU PE/36/2018/REV/1, *OJ L* 312, 7.12.2018, pp. 56-106. Note that what the SIS II package refers to as "dactyloscopic data" in Article 3(14) of Regulation (EU) 2018/1861 and 3(13) of Regulation (EU) 2018/1862 includes fingerprints and palm prints.

¹⁴⁰ As required in accordance with Articles 24 (5), 43 (3) and 50 (5) of Regulation (EC) No. 1987/2006 and Articles 59 (3) and 66 (5) of the Council Decision 2007/533/JHA – see the Council of the EU, *Report from the commission to the European Parliament and the Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and art. 59 (3) and 66 (5) of Decision 2007/533/JHA*, 15810/16, Brussels, 23 December 2006, as well as the Council of the EU, *Commission Staff Working Document ,Accompanying the document Report from the Commission to the European Parliament and the Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with articles 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and articles 59 (3) and 66 (5) of Decision 2007/533/JHA*, 15810/16 ADD 1, Brussels, 23 December 2006.

¹⁴¹ See the eu-LISA, *Report on the technical functioning of Central SIS II and the Communication Infrastructure, including the security thereof and the bilateral and multilateral exchange of supplementary information between Member States*, Tallin, 2015, available at www.eulisa.europa.eu. On eu-LISA, see Chapter 4.

¹⁴² Proposal for a Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third-country nationals, COM(2016) 0881 final, Brussels, 21.12.2016.

¹⁴³ Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006, COM(2016) 0882 final, Brussels, 21.12.2016.

¹⁴⁴ Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No. 515/2014 and repealing Regulation (EC) No. 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU*, 15814/16, Brussels, 23 December 2006.

to the EDPS, the existence of the SIS II copies was due to the bizarre architecture that characterises the SIS II. In his words:

‘The current and proposed architecture of SIS is neither centralised nor decentralised but a mix that inherits the weaknesses of both: as the information is pooled together by all participating Member States, all SIS information is available to all Member States in their national copies and to eu-LISA in the central system (as if all SIS copies were a central system). Because the information is replicated in all different copies, the information in SIS is as secure as the less secure of any of the national copies’¹⁴⁵.

In the end, Member States were granted the possibility to decide whether to maintain a national copy or not, and may also decide to share their data with each other. This is especially relevant for some small Member States – e.g., Slovenia – that have never been able to implement national copies as they only integrated into the system recently, in the 2000s.

The three proposals aimed at introducing several major new features: SIS II alerts on irregular migrants who were subject to return decisions; the use of facial images for biometric identification, in addition to fingerprints; the automatic transmission of information on a hit following a check; the storing of hit information on discreet, inquiry, and specific check alerts in the SIS Central System, and the creation of a new alert category on “Wanted Unknown Persons” for which forensic data may exist in national databases. Furthermore, new provisions to enhance the security features were positively evaluated by the EDPS while focusing on how security incidents can lead to data breaches and that there was a need to minimise the adverse consequences. The EDPS especially appreciated the new rules on: data quality; statistics, business continuity plan and incident reporting; the obligation to conduct regular trainings on data security and data protection for the staff authorised to have access to the SIS II; the mechanism for deleting the alerts, as well as Europol’s access to the SIS II.

As a general rule, alerts are kept as long as deemed necessary to achieve the purposes for which they were entered¹⁴⁶. The Regulations set deadlines for the revisions of alerts which vary depending on the legal framework and whether the alert concerns a person or an object¹⁴⁷. The end of the data retention period was standardised as up to five years for the majority of alerts and was criticised in the light of the new CJEU case law that seeks to provide specific rules on the retention period depending on the categories of data ‘[...] on the basis of their possible

¹⁴⁵ See the Council of the EU, *Opinion 7/2017 on the new legal basis of the Schengen Information System*, 9412/17, Brussels, 17 May 2017, p. 14.

¹⁴⁶ See Article 39(1) of Regulation (EU) 2018/1861 and Article 53(1) of Regulation (EU) 2018/1862.

¹⁴⁷ Regulation (EU) 2018/1861 provides for an ordinary review period of three years unless the national decision on which the person’s alert is based provides for a longer period of validity, in which case it shall be reviewed after five years – see recital (31). For its part, Article 53 of Regulation (EU) 2018/1862 provides for different review deadlines depending on the holder of the alert.

usefulness for the purposes of the objective pursued or according to the persons concerned'¹⁴⁸. However, the deletion may also occur in specific cases related to the categories of data processed. For example, alerts for surrender or extradition purposes are deleted when the person has been surrendered or extradited to the competent authorities of the issuing Member State, or when the judicial decision is revoked¹⁴⁹. Along the same lines, alerts on missing or vulnerable persons are deleted when the person has been located¹⁵⁰. Finally, alerts on return shall be deleted:

- as soon as the return is complied with, or there is sufficient and convincing information that the third-country national has left the territory of the Member State;
- the decision on the basis of which the alert was issued has been revoked or annulled by the competent authority;
- the third-country national can demonstrate that s/he has left the territory of the Member State in compliance with the relevant return decision, or
- the person has acquired the nationality of a Member State, or of any state whose nationals enjoy the right to free movement under EU law¹⁵¹.

Apart from these considerations, each SIS II Regulation provides for new types of alerts that are worth separate analysis.

2.2.1. The new second generation of the SIS on refusal of entry

Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation, and use of the SIS in the field of border checks was adopted on the basis of the EU powers set forth in Article 77(2)(b) and (d) TFEU on border checks and the progressive implementation of an integrated border management system, as well as Article 79(2)(c) TFEU on irregular migration. Hence, with respect to its previous framework, significant changes have been made, including: the lack of reference to the current Article 74 TFEU, and the insertion of a new legal basis on the integrated border management strategy set forth by the Lisbon Treaty under Article 77(2)(d) TFEU.

The use of the SIS II for refusal of entry alerts was problematic from the very beginning of the SIS, since Member States were reported to interpret the regulation differently and, as a consequence, to adopt different practices, hindering a fluent exchange of information.

¹⁴⁸ See the C-293/12 and C-594/12, *Digital Rights Ireland Ltd (C-293/12) v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General*, 8 April 2014, EU:C:2014:238, para. 63.

¹⁴⁹ See Article 55(1) of the Regulation (EU) 2018/1862.

¹⁵⁰ See Article 33(4) of Regulation (EU) 2018/1862.

¹⁵¹ See Article 14 of the Regulation (EU) 2018/1860.

Therefore, the SIS II recast Regulation (EU) 2019/1861 to oblige Member States to issue entry ban alerts in case a third country national is found to be irregularly staying in the territory of the Member States in accordance with the Return Directive¹⁵². As a result, an entry ban alert shall be issued when:

- a third country national poses a threat to public policy, public security or national security, or
- when the decision for an entry ban is issued in accordance with the Return Directive¹⁵³.

In the former examples, alerts shall be based on a judicial or administrative decision of a Member State which, in accordance with its national law, considers the presence of the third-country national to be posing a threat to public policy or national security and therefore prevents him/her from entering and staying in its territory. The scenario covers three different types of situations¹⁵⁴, of which only one is new: third-country nationals that have circumvented, or attempted to circumvent, EU or national rules on entry and staying in the territory of the Member States¹⁵⁵. In the latter case, an entry ban shall be issued in accordance with the Return Directive¹⁵⁶, the new Article 13 of the recast proposed Return Directive, for which entry ban alerts are issued when no period for voluntary departure has been granted, or the obligation to return has not been complied with. It shall be noted that in light of the recast Proposal for a Return Directive¹⁵⁷, entry ban alerts will also be issued together with the return decision at the time of leaving the territory of a Member State, as well as when the third-country national is found to be irregularly staying in the Member States' territories¹⁵⁸.

¹⁵² See Article 11 of the Return Directive.

¹⁵³ See Article 24(1) of Regulation (EU) 2018/1861. In its second paragraph, this Article specifies under which circumstances Member States may evaluate the existence of a threat to public policy, to public security or to national security.

¹⁵⁴ With regard to Regulation (EC) No 1987/2006, this provision maintains the case of a third-country national convicted of an offence involving deprivation of liberty of at least one year, and the case where there are "serious grounds" for believing that a third-country national has committed or is suspected of committing a serious crime on the territory of a Member State, including the terrorist offence – it should be pointed out that it changes the wording of Article 24(2)(b) of Regulation (EC) No 1987/2006 which required "serious reasons".

¹⁵⁵ See Article 24(2)(c) of Regulation (EU) 2018/1861. These are all cases where the third-country national violates an EU or national rule on entry and stay in the territory which constitutes an administrative offence. For example, all those remaining in the Schengen area after the expiry of the maximum period of stay of their visa or residence permit, as well as all returns at border crossing points that prevent aliens from entering the territory.

¹⁵⁶ See Articles 11 of the Return Directive.

¹⁵⁷ Proposal for a Directive of the European Parliament and of the Council on common standards and procedures in Member States for returning illegally staying third-country nationals (recast), COM(2018) 634 final, Brussels, 12.9.2018. A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018, COM(2018) 634 final, Brussels, 12.09.2018 (hereinafter recast Proposal for a Return Directive).

¹⁵⁸ See Article 13(2) of the recast Proposal for a Return Directive. In addition, a final situation in the case of a third-country national is subject to a restrictive measure adopted by the Council, including a travel ban of the United Nations Security Council – Article 25 of Regulation (EU) 2018/1861. The description is introduced by the Member State holding the Presidency of the Council of the EU at the time of adoption of the measures.

In the second instance, the Regulation on refusal of entry alerts introduces a system of mandatory queries between Member States to prevent a person registered in the SIS II from being able to legally enter and stay in another Member State. Cooperation between Member States is deployed through the SIRENE Platform¹⁵⁹ that enables the exchange of supplementary information – i.e., information which is not part of the data of an alert stored in SIS, but which relates to the SIS alerts. This mechanism is firstly triggered by the Member State wishing to grant or extend a residence permit or long-stay visa to a third-country national who is the subject of an alert in the SIS II. For this purpose, Member States are now obliged to consult the SIS II, including the Member State issuing the alert¹⁶⁰. Second, the Member State that wants to issue an SIS II alert prohibiting the entry and residence of a third-country national holding a valid residence permit or long-stay visa shall consult the Member State that granted the third-country national the right to stay in its territory¹⁶¹.

2.2.2. The new second generation of the SIS on return

Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals¹⁶² was adopted on the basis of the EU policy on the prevention of, and fight against, irregular migration, namely Article 79(2)(c) TFEU.

During the negotiations for Regulation (EU) 2018/1860, the Council Legal Service maintained that alerts on return should have been conceived as a development of the Schengen *acquis* and not as a concretisation of the EU's illegal migration policy¹⁶³. As a consequence, it suggested the merger of both Regulations (EU) 2018/1860 and (EU) 2018/1861 under a unique legislative act underpinned by Article 79(2)(c) and Article 79(2)(d) TFEU. Indeed, the EU return policy was conceived as a hybrid act: some of its dispositions may be traced back to the Convention implementing the Schengen Agreement, while others stem from EU policy on

¹⁵⁹ The SIRENE Bureaux will have to be operational twenty-four hours a day and seven days a week to ensure the exchange and availability of all supplementary information. For this purpose, each SIRENE Bureau has access not only to the SIS II data but also to all national information concerning alerts in its Member State. The top priority requests for information are qualified as “urgent” and the reasons for this urgency are specified. On the exchange of information through the SIRENE channel, see the Commission Implementing Decision (EU) 2017/1528.

¹⁶⁰ See Article 27 of Regulation (EU) 2018/1861.

¹⁶¹ See Article 29 of Regulation (EU) 2018/1861.

¹⁶² Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals, PE/34/2018/REV/1, OJ L 312, 7.12.2018, pp. 1-13.

¹⁶³ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third-country nationals - Schengen relevance*, 10768/17, Brussels, 28 June 2017.

irregular migration¹⁶⁴. The same reasoning would be applicable to the SIS II alerts on refusal of entry, which have always raised some inconsistencies with the founding Treaties. This interpretation has huge consequences on Member States' participation in the relevant instruments – namely, the Return Directive and its concretisation in the SIS II alerts – as we will further address in Chapter V when dealing with variable geometry *vis-à-vis* large-scale IT systems and the interoperability framework.

The SIS II alerts on return implement the Return Directive with the Council Directive 2001/40/EC on the mutual recognition of decisions on the expulsion of third country nationals¹⁶⁵. According to the Council Directive 2001/40/EC, Member States can recognise the return decision issued by another Member State so as to execute the return of the third country national irregularly staying in the Member States' territories or apprehended while irregularly crossing the external borders in breach of the Schengen Borders Code¹⁶⁶. The Regulation obliges Member States to enter a new type of SIS II alert when issuing a return decision and in order to verify the compliance with the return procedure¹⁶⁷. In this sense, entry ban alerts and return alerts are incompatible but complementary: the return alert shall be issued together with the return decision and, if an entry ban decision is expedited, the SIS II alert on return shall be turned into an SIS II alert on refusal of entry once the return has been executed. The insertion of return alerts into the SIS II is a rather significant change in the light of the nature of the system as it shifts from the criminal area to the prevention of and fight against irregular migration. The reform significantly expands the alerts that will be stored in the SIS II for administrative purposes by covering all cases of return, with or without an entry ban alert¹⁶⁸, including those cases where the migrant is leaving through the EU's external borders¹⁶⁹.

In order to achieve its goals, Regulation (EU) 2018/1860 establishes a cooperation mechanism among competent authorities in order to identify those third-country nationals who are subject to a return decision, who have absconded and have been apprehended in other

¹⁶⁴ *Ibid.*, p. 34.

¹⁶⁵ *Ibidem*.

¹⁶⁶ See Article 13 of the Schengen Borders Code.

¹⁶⁷ See Article 3 of Regulation (EU) 2018/1860.

¹⁶⁸ Where a return decision is accompanied by a refusal of entry and stay, or the third-country national does not comply with the return decision, Member States should immediately activate the alert in SIS II on the basis of a copy of the negative decision – see recitals (15) and (16) of Regulation (EU) 2018/1860.

¹⁶⁹ In case of “hits” at exit, the executing Member State should contact the issuing Member State to inform it of the specific circumstances and confirm the return – see Article 6 of Regulation (EU) 2018/1860. It is up to the issuing Member State, indeed, to cancel the alert recorded in SIS II. If a return alert is issued in time, the executing State should inform the issuing Member State in order to delete the alert on return and maintain, where appropriate, the alert for refusal of entry and stay, as a result of which the subject complied with its obligation to leave the territory of the Member State.

Member States, for which supplementary information can be exchanged via the SIRENE Platform. These mechanisms come into use when:

- a Member State wants to enter an alert on return though the third-country national holds a valid residence permit or long-stay visa issued by another Member State¹⁷⁰;
- a Member State wants to grant or extend a residence permit or long-stay visa to a third-country national subject to a return decision of another Member State¹⁷¹, and
- a hit is reported on an alert on return entered by a Member State with respect to a third-country national holding a valid residence permit or long-stay visa granted by another Member State¹⁷².

The authorities that have access to the SIS II for the purpose of entering, updating, deleting, and searching alerts are those competent to issue and enforce a return decision in accordance with the Return Directive¹⁷³. In addition, return alerts can be accessed by the following national authorities: those competent for the identification of third-country nationals according to Regulation (EU) 2018/1861¹⁷⁴; those competent for naturalisation¹⁷⁵; national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charging an individual¹⁷⁶; Europol for the prevention and combating of migrant smuggling and irregular migration¹⁷⁷, and the EBCG Agency's teams for the purpose of carrying out border checks, border surveillance, and return operations¹⁷⁸.

2.2.3. The new second generation of the SIS on police and judicial cooperation in criminal matters

Regulation (EU) 2018/1862 brings in important additions to the SIS II as far as criminal law is concerned on the basis of Articles 82(1)(d), second subparagraph, 85(1), 87(2)(a) and 88(2)(a) of the TFEU.

First of all, a new category of alerts, labelled as “preventive alerts”, has been established in order to prevent missing persons, children at risk, and vulnerable persons from travelling¹⁷⁹. In

¹⁷⁰ See Articles 10 and 11 of Regulation (EU) 2018/1860.

¹⁷¹ See Article 9 of Regulation (EU) 2018/1860.

¹⁷² See Article 12 of Regulation (EU) 2018/1860.

¹⁷³ See recital (19) of Regulation (EU) 2018/1860.

¹⁷⁴ Article 34(1) of Regulation (EU) 2018/1861.

¹⁷⁵ Article 34(2) of Regulation (EU) 2018/1861.

¹⁷⁶ Article 34(3) of Regulation (EU) 2018/1861.

¹⁷⁷ See Article 17(2) of Regulation (EU) 2018/1860.

¹⁷⁸ See Article 17(3) of Regulation (EU) 2018/1860.

¹⁷⁹ See Article 32 of Regulation (EU) 2018/1862.

the case of missing persons, Regulation (EU) 2018/1862 includes the possibility to collect DNA profiles after the execution of a data quality check¹⁸⁰. This does not only concern the DNA of the missing person, but also the DNA of his/her family members that can be added to the database with their consent¹⁸¹. The EDPS recommended that the DNA profiles should not contain information, like the individual's racial origin or any other sensitive information¹⁸². We believe that it would be better to insert a provision on proportionality that ensures that such highly sensitive biometrics can only be inserted when photographs, facial images or dactylographic data are not available. This new category of alerts will be especially relevant to children at risk of parental abduction, of becoming victims of trafficking, or of being enlisted in armed groups and should be welcomed. The issuing of the alert is based on the decision of a competent national authority, including judicial authorities, in charge of parental custody. In this sense, the SIS II will support the implementation of the Council Regulation (EC) No 2201/2003 of 27 November 2003 concerning jurisdiction and the recognition and enforcement of judgments in regard to matrimonial and parental responsibility, repealing Regulation – commonly known as Brussels II bis¹⁸³.

The obligation to create alerts on subjects regarding terrorism-related activities has been strengthened through the insertion of a new category of alerts on “unknown wanted persons”¹⁸⁴. This alert shall be based on the insertion of fingerprints or palm prints discovered at the scene of terrorist offences or other serious crimes under investigation, i.e. latent prints, for the purposes of biometric identification. In case of a hit, the identity of the person shall be established on the basis of national law, though the Member State issuing the alert shall be informed through the exchange of supplementary information¹⁸⁵.

Third, a new alert for inquiry checks for the purposes of contrasting terrorism and serious crimes will enable police authorities to stop and question the person concerned. An inquiry check is defined as the power of police authorities to “stop and search” which is generally

¹⁸⁰ See Article 42(3) of Regulation (EU) 2018/1862.

¹⁸¹ See Article 42(3) of Regulation (EU) 2018/1862.

¹⁸² See the Council of the EU, 9412/17, Brussels, 17 May 2017, p. 9.

¹⁸³ Council Regulation (EC) No 2201/2003 of 27 November 2003 concerning jurisdiction and the recognition and enforcement of judgments concerning jurisdiction and the recognition and enforcement of judgments in matrimonial matters and the matters of parental responsibility, repealing Regulation (EC), No 1347/2000, *OJ L* 338, 23/12/2003, p. 1.

¹⁸⁴ See Article 40 of Regulation (EU) 2018/1862 and also the Council of the EU, *Draft Council Conclusions - Strengthening the cooperation and the use of the Schengen Information System (SIS) to deal with persons involved in terrorism or terrorism-related activities, including foreign terrorist fighters - Adoption*, 8974/18, Brussels, 18 March 2018.

¹⁸⁵ Council of the EU, 12661/16, Brussels, 3 October 2006, p. 6: ‘This will be assessed with a view to seeking complementarity and avoiding overlap with the existing Prüm framework for searching fingerprints in the different national databases of EU Member States’.

regulated differently in each Member State. For this reason, Member States that did not foresee this possibility in their national system were invited to harmonise their national law accordingly¹⁸⁶.

Finally, to strengthen the Member States' cooperation between police and criminal judicial authorities, during the negotiations the possibility of inserting new alerts for the purposes of the European Investigation Order was also suggested, along with the mutual recognition of criminal judgments¹⁸⁷, and financial penalties¹⁸⁸. However, these new types of alerts were not integrated into the final legislative text.

Regulation (EU) 2018/1862 also allows for the exchange of supplementary information, yet this information depends on the underlying case that legitimises the insertion of data in the SIS II¹⁸⁹.

¹⁸⁶ See the Council of the EU, *Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU - draft compromise text regarding alerts on persons and objects for discreet checks, inquiry checks or specific checks (Articles 36 and 37)*, 8411/17, Brussels, 26 April 2017.

¹⁸⁷ Council Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union, as amended by Council Framework Decision 2009/299/JHA of 26 February 2009, *OJ L* 327, 5.12.2008, pp. 27-46.

¹⁸⁸ Council Framework Decision 2005/214/JHA of the 24 February 2005 on the application of the principle of mutual recognition to financial penalties as amended by Council Framework Decision 2009/299/JHA of 26 February 2009, *OJ L* 76, 22.3.2005, pp. 16-30.

¹⁸⁹ See Articles 7 and 8 of Regulation (EU) 2018/1862.

3. European Asylum Dactyloscopy system (Eurodac)

The European Asylum Dactyloscopy system (Eurodac) was implemented in 2000¹⁹⁰ on the basis of Article 63(1)(a) of the TEC¹⁹¹ to support the Dublin Convention¹⁹². Both instruments

¹⁹⁰ See the Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, *OJ L* 316, 15.12.2000, pp. 1-10 (2000 Eurodac Regulation hereinafter). Eurodac negotiations started in the intergovernmental framework under the ex-first pillar according to Article K.1(1) of the 1992 TEU that empowered the Council to adopt intergovernmental measures set forth in Article K.3 in the field of asylum. See the Council of the EU, *Draft Convention concerning the establishment of "Eurodac" for [the taking, recording], comparison [and exchange] of fingerprints of applicants for asylum*, 101/97, Brussels, 15 September 1997. The adoption of the Eurodac Convention and its relevant Protocol on third country nationals founded irregularly crossing the external borders started at the beginning of the '90s on the basis of Article 15 of the Dublin Convention and were subsequently taken in charge by the JHA Council since 1995. On the elaboration of the Eurodac Convention and its relevant Protocol on irregular migrants see Evelien Brouwer, 2008, *op. cit.*, pp. 118-121, who notes how the legislative works slowed down in view of the entry into force of the Amsterdam Treaty in 1999. On the institutionalisation of Eurodac consult the document of the EU Council of the EU, *Eurodac implementing rules*, 8140/99, Brussels, 11 May 1999, and Mascia Toussaint, "EURODAC: un système informatisé européen de comparaison des empreintes digitales des demandeurs d'asile", *Revue du marché commun et de l'Union Européenne*, No. 429, 1999, pp. 421-425. Brigitta Kuster, "How to Liquefy a Body on the Move: Eurodac and the Making of the European Digital Border", in Raphael Bossong, and Helena Carrapico, *EU Borders and Shifting Internal Security*, Cham, Springer, pp. 45-63, on the contrary, analyses the contribution of Eurodac to the digitalisation of EU external borders.

¹⁹¹ Now Article 78(2)(e) of the TFEU.

¹⁹² Despite the fact that some provisions on the responsibility for processing an asylum application were also agreed under Articles 28-38 of the Convention implementing the Schengen Agreement, the criteria were recollected in the Dublin Convention agreed on the 15 June 1990 whose entered into force was postponed until a sufficient number of rectifications was achieved – see the Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities, *OJ C* 254, 19.8.1997, pp. 1-12 (Dublin Convention). The Dublin Convention was substituted by the Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, *OJ L* 50, 25.2.2003, pp. 1-10 (Dublin Regulation) that has been repealed in 2013 by Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person, *OJ L* 180, 29.6.2013, pp. 31-59 (Dublin II Regulation hereinafter). Two amended proposals have been presented by the European Commission in 2016: the Proposal for a Regulation of the European Parliament and of the Council establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast), COM(2016) 0270 final, Brussels, 4.5.2016, and the Proposal for a Regulation of the European Parliament and of the Council on asylum and migration management and amending Council Directive (EC) 2003/109 and the proposed Regulation (EU) XXX/XXX [Asylum and Migration Fund], COM(2020) 610 final, Brussels, 23.9.2020; the latter is titled "Asylum and Migration Management Regulation". On the Dublin Convention see Clotilde Marinho, *The Dublin Convention on Asylum: its essence, implementation and prospects*, Maastricht, European Institute of Public Administration, 2000; Agnes Hurwitz, "The 1990 Dublin Convention: A Comprehensive Assessment", *International Journal of Refugee Law*, Vol. 11, 1999, pp. 646-677; Karen Birchard, "Dublin Convention on handling of EU asylum seekers becomes law", *The Lancet (British edition)*, Vol. 350, 1997, pp. 675-748; Concepción Escobar Hernández, "El convenio de aplicación de Schengen y el Convenio de Dublín: una aproximación al asilo desde la perspectiva comunitaria", *Revista de instituciones europeas*, 1993, pp. 53-100; Giovanni Barontini, "Sulla competenza per l'esame delle domande di asilo secondo le convenzioni di Schengen e Dublino", *Rivista di Diritto Internazionale*, Vol. 75, No. 2, 1992, pp. 335-347, and Cláudia Faria, *The Dublin Convention on Asylum: between reality and aspirations*, Maastricht, European Institute of Public Administration, 2001, and Wenceslas de Lobkovic, "La Convention de Dublin: un utile complément au droit humanitaire international", *Objectif Europe*, No. 10, 1990, pp. 7-12.

were integrated the so-called Dublin system¹⁹³ whose major purpose was to detect asylum seekers in order to avoid the so-called “asylum shopping” – i.e., the possibility to submit more than one application for asylum to different Member States¹⁹⁴. Assuming that most applicants would lack valid document, the collection of biometrics seemed to be an immediate and effective solution to identify asylum applicants and irregular migrants¹⁹⁵. These instruments were introduced into the Eurodac negotiations in order to give effectiveness to one of the criteria of responsibility. According to this criterion, the Member State whose borders were illegally crossed should be responsible for examining the (eventual) subsequent asylum application¹⁹⁶.

In the case of irregular migrants, data has to be stored for a period of two years – now eighteen months¹⁹⁷ – while asylum applicants have their fingerprints registered for a period of

¹⁹³ On the institutionalisation of the Dublin system see Reinhard Marx, “Adjusting the Dublin Convention: New Approaches to Member States Responsibility for Asylum Applicants”, *European Journal of Migration and Law*, 2001, Vol. 3, No. 1, pp. 7-21, and Catherine Phoung, “The Dublin Convention on Asylum: Its Essence, Implementation and Prospects”, *European Public Law*, Vol. 7, 2001, pp. 325-327.

¹⁹⁴ Evelien Brouwer, 2008, *loc. cit.*, highlights that Dublin did not want to implement a freedom of movement area yet, in my view, it is difficult to support another rationale as the EU Council’s Legal Service defended in Council of the EU, *Opinion on the Possibility of including data on illegal migrants in the Eurodac system*, 5754/98, Brussels, 16 March 1998, p. 2. By setting minimum criteria of responsibility, asylum applicants should have been ensured to have the application examined.

¹⁹⁵ See recital (4) of the 2000 Eurodac Regulation for which: ‘Fingerprints constitute an important element in establishing the exact identity of such persons. It is necessary to set up a system for the comparison of their fingerprint data’. On the use of biometrics as a form of control of migration flow, see Jonathan P. Aus, *Supranational governance in an “area of freedom, security and justice”: Eurodac and the politics of biometric control*, Sussex, Sussex European Institute, 2003.

¹⁹⁶ Although the Council Legal Service clearly stand out that this should have strictly include persons having found crossing a Member States frontiers illegally, the interpretation given by the Member States enlarged its scope of application beyond the external borders, when the person would have been found *en route*. See the opinion of the Council of the EU, 5754/98, 16 March 1998, p. 10, and the Council of the EU’s documents: *Fingerprinting of illegal immigrants: Feasibility study of the possible extension of the Eurodac Convention*, 7566/98, Brussels, 8 April 1998, as well as the *Draft Council Act drawing up a Protocol extending the scope rationae personae of the Convention on the establishment of “Eurodac” for the comparison of fingerprints of applicants for asylum*, 6324/99, Brussels, 4 March 1998. A final version was agreed so that fingerprints of irregular migrants apprehended while illegally crossing a Member State’s border could have been compare only with subsequent asylum applications recorded in the Eurodac Central Unit, see Article 9 of the 2000 Eurodac Regulation. However, Member States could have transmitted to the Eurodac Central Unit also the data of migrants irregularly found within the territory of the State – see the Council of the EU, *First annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit*, 9319/04, Brussels, 13 May 2004, p. 6.

¹⁹⁷ See further *infra* on Article 16(1) of the 2013 Eurodac recast Regulation. However, the European Commission Proposal aimed at one year only in accordance with the one-year period established for the responsibility of taking in charge the migrants by the Member States of access would have ceased according to current Article 13(1) of the Dublin III Regulation. The timeline period for storing irregular migrant’s data was a sensitive topic during the negotiations that could be agreed only in the triologue. Confront the Council of the EU: *Proposal for a Regulation of the European Parliament and of the Council concerning the establishment of ‘Eurodac’ for the comparison of fingerprints for the effective application of Regulation (EC) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person]*, Annex, 16934/08, Brussels, 9 December 2008, pp. 3 and 4, with the following *Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of ‘EURODAC’ for the comparison of fingerprints for the effective application of Regulation (EU) No [...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States’ law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No*

ten years¹⁹⁸. Alongside these two categories of persons, a provision on migrants irregularly found in a territory of the Member States was also inserted, and their fingerprints could be crosschecked with the Eurodac but not stored therein¹⁹⁹.

The Eurodac was the pioneering large-scale IT system for the storage of fingerprint data in a small biometric matching system provided with the AFIS²⁰⁰. Although fingerprints have always constituted the focal point of the Eurodac, it is important to recall that the Central System also stores a limited amount of alphanumeric data²⁰¹ and, first and foremost, that Member States are allowed to share further information through the DubliNet communication network – usually by emails²⁰². During the discussions around the implementation of the AFIS this gave

1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version), 11861/12, Brussels, 6 June 2012, p. 55, and the *Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version) - Analysis of the final compromise text with a view to an agreement*, 7713/13, Brussels, 25 March 2003.

¹⁹⁸ See respectively Articles 6 and 10 of the 2000 Eurodac Regulation.

¹⁹⁹ Article 10 of the 2000 Eurodac Regulation.

²⁰⁰ This form of recognition is also known as one-to-many match since the data of one individual that want to be identified is compared with all the data stored in a database that belongs to other persons. The level of accuracy of the AFIS in the Eurodac was positively estimated as for the False Positive (FPR) and False Negative Rates (FNR) already in 2009 when the European Commission reported that:

'One "false hit" – i.e., wrong identification performed by the AFIS, was reported in 2007, being the first false hit reported from a ten-print search in the Eurodac since the beginning of the activities of the system. Although Member States are required to verify all hits immediately, as described in Article 4(6) of the 2000 Eurodac Regulation, they are currently not obliged to notify the Commission of false hits. However, with one false hit reported out of more than 1.1 million searches and more than 200.000 hits the system can still be considered extremely accurate'.

See the Communication from the Commission to the European Parliament and the Council - Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2007, COM(2009) 0013 final, Brussels, 26.1.2009. Despite this, it shall be highlighted that under the 2000 Eurodac Regulation, Member States did not have any obligation to report the FPR and the FNR to the European Commission that, on that time, was in charge of the Eurodac Central Unit.

²⁰¹ Confronting Article 11 of the 2013 Eurodac recast Regulation with Article 5 of the 2000 Eurodac Regulation; the former introduced the following information: operator user identification; where applicable in accordance with Article 10(a) or (b), the date of the arrival of the person concerned after a successful transfer; where applicable in accordance with Article 10(c), the date when the person concerned left the territory of the Member States; where applicable in accordance with Article 10(d), the date when the person concerned left or was removed from the territory of the Member States; where applicable in accordance with Article 10(e), the date when the decision to examine the application was taken. On the contrary, references to the date on which the data were transmitted to the Central Unit, the date on which the data were entered in the central database, and the details in respect of the recipient(s) of the data transmitted and the date(s) of transmission(s) have been canceled.

²⁰² Commission Regulation (EC) No 1560/2003 of 2 September 2003 laying down detailed rules for the application of Council Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, *OJ L* 222, 5.9.2003, pp. 3-23. On the need of data protection rules as for the data exchanged through DubliNet see the Opinion of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council, COM(2008) 820 final, Brussels, 23.9.2009, paras. 24-33, and Franziska Boehm, *Information Sharing and*

rise to an important debate about the technical feasibility and ethics of processing biometric data, with special emphasis on the protection of children's rights²⁰³.

Given that refugees are viewed as a vulnerable group, the Eurodac has always raised concerns regarding their fundamental rights. In addition, asylum constitutes a delicate political matter for Member States and they are called on to support each other in the light of the principle of solidarity²⁰⁴ under the 2007 Lisbon Treaty. As a consequence, the negotiations of the recast Regulation adopted in 2013 and the one that began in 2016 have been long and particularly challenging.

3.1. The 2013 Eurodac recast Regulation

The 2000 Eurodac Regulation was significantly recast in 2013, after a long period of negotiations in which three different proposals were submitted by the European Commission:

- the first in December 2008²⁰⁵;
- the second in September 2009²⁰⁶, and
- the third, final proposal in May 2012²⁰⁷.

Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level, Luxembourg, Springer, 2012, pp. 304-314.

²⁰³ The Eurodac stores biometrics from the minimum age from of fourteen years old which was justified in the light of the right to family reunification. During the Eurodac negotiation of 2013, a proposal to lower the limit age to twelve years old was presented in alignment with the VIS Regulation – see the Council of the EU, *Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (recast)*, 7649/09, Brussels, 2 April 2009, p. 13. Laurent Beslay, Javier Galbally Herrero, and Rudolf Haraksim, *Automatic fingerprint recognition: from children to elderly. Ageing and age effects*, JRC Technical Report, Italy, 2018, stand out that the major obstacle to detect children's fingerprints is related to their physical characteristics that change significantly. Nevertheless, the new technique allows for the detection of fingerprints since the twelve years old.

²⁰⁴ See Article 80 of the TFEU.

²⁰⁵ See the Proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (Recast version), COM(2008) 825 final, Brussels, 4.5.2016.

²⁰⁶ See the Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No. [...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version), COM(2012) 0254 final, Brussels, 4.5.2016.

²⁰⁷ See the Council of the EU, *Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011*

The first proposal presented in December 2008²⁰⁸ aimed at addressing the data protection deficiencies that had been reported by the supervisory bodies since the early 2000s²⁰⁹. Soon after it was put into motion, the Eurodac was reported as being misused through the undertaking of “special searches” by virtue of Article 18(2) of the 2000 Eurodac Regulation. It is not clear what these special searches were, but based on the European Commission evaluation²¹⁰, it seems that authorities other than the data subjects were querying the system so as to retrieve asylum seekers’ data. The European Commission denounced the margin of manoeuvre given to the Member States to adopt an undefined list of authorities with access to the system as a crucial obstacle in detecting these “special searches”. This issue was addressed in the Eurodac recast Regulation of 2013 that obliged Member States’ authorities to keep a written record of the data subject’s requests to access his/her own information²¹¹. Moreover, Member States were required to submit a list of designated and verifying law enforcement authorities with access to the Eurodac²¹². Although the number of “special searches” has decreased since the first

establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version), 10638/12, Brussels, 4 June 2012.

²⁰⁸ See the Proposal for a Regulation of the European Parliament and of the Council, COM(2008) 825 final, Brussels, 4.5.2016.

²⁰⁹ According to Article 24(1) of the Eurodac Regulation 2000 the European Commission published the following Eurodac Annual reports: Commission Staff Working Paper, First annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit, SEC(2004) 557, Brussels, 5.5.2004; Commission Staff Working Paper, Second annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit, SEC(2005) 839, 20.05.2005; Commission Staff Working Paper, Third annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit, SEC(2006), 21.11.2006; Council of the EU, *Fourth annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit*, 12928/07, Brussels, 14 September 2007; Report from the Commission to the European Parliament and the Council, Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2008, COM(2009) 494 final, 25.9.2009; Report from the Commission to the European Parliament and the Council, Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2008, COM(2009) 13 final, 26.1.2009; Report from the Commission to the European Parliament and the Council, Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2008, COM(2010) 415 final, 3.08.2010; Report from the Commission to the European Parliament and the Council, Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2008, COM(2011) 549 final, 12.09.2011; Report from the Commission to the European Parliament and the Council, Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2008, COM(2012) 533 final, 21.09.2012, and Report from the Commission to the European Parliament and the Council, Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2008, COM(2013) 485 final, 28.06.2013.

²¹⁰ In the Council of the EU, *Second annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit*, 10464/05, Brussels, 23 June 2005, p. 15, the European Commission assessed that ‘[w]hile a number of these requests could be attributed to the raise awareness of data protection principles in the early days of EURODAC, it should be reminded that the use of Article 18 is legally limited to the requests for access to personal data by individuals’ and declared to be determined to taking steps against Member States misusing the system’. This was also recalled in the Council of the EU, 12928/07, Brussels, 14 September 2007, p. 6, where the European Commission specified to have warned the EDPS on this issue.

²¹¹ Article 29(11) of the 2013 Eurodac recast Regulation.

²¹² Article 43 of the 2013 Eurodac recast Regulation.

European Commission report, some confusion on the effectiveness of these new provisions still remains²¹³.

Another important element of the discussion in the early '2000s concerned the 'blocking' of refugees' data. The 2000 Eurodac Regulation imposed the 'blocking' of the data of those individuals registered in the Eurodac to whom refugee status would have been granted. In practice, the 'blocking' of data was only visible to the Member States granting the protection, but other Member States could still search the refugee's personal data without being aware of the change of status, breaching the principle of purpose limitation. Along the same lines, this blocking tool was preventing Member States from seeing whether a beneficiary of international protection had lodged another asylum application in a different Member State²¹⁴. As a result, the European Commission proposed to either insert another category of data on refugees (CAT4), or to store refugees' fingerprints²¹⁵. The latter suggestion was welcomed in the 2013 Eurodac recast Regulation which finally inserted a provision on "marking" the data of individuals to whom international protection was granted²¹⁶. However, this means that another category of migrants has their data stored in the system for a period of three years, even though international protection has been granted²¹⁷.

In the early 2000s, discussions pivoted around the so called "advanced data erasure" strategy that sought to delete the data of asylum applicants following the granting of EU citizenship, a residence permit, or the execution of a return decision. The lack of communication among the Member States prevented them from seeing whether the data had been deleted on one of these grounds and, consequently, fingerprints were found to be stored for a longer period than the one envisaged by the Regulation. A first initiative of the European Commission contemplated different means of addressing this issue, among which were: the use of DubliNet as a bilateral communication channel; the transformation of DubliNet itself into a centralised system, and an automated notification system stemming from the Eurodac Central Unit. The situation was further examined by the Eurodac Supervision Coordination Group that suggested the

²¹³ See the Council of the EU, *Annual report on the 2013 activities of the Central Unit of Eurodac pursuant to Article 24(1) of Regulation (EC) No 2725/2000*, 10898/14, Brussels, 12 June 2014, p. 12, in which the Agency stands out that on forty-nine special searches, thirty-four were launched by France '[...] due to proactive NGOs in the Calais region encouraging data subjects to request such searches'.

²¹⁴ What is strange is that the European Commission later on admitted that the rate of "multiple asylum applications" was altered since Member States were inserting new records each time an asylum applicant was taken back on the basis of the Dublin regulation so the statistics on which it was relying its assumptions were not fully valid.

²¹⁵ See the Council of the EU, 7649/09, Brussels, 2 April 2009, p. 27.

²¹⁶ See Article 18 of the 2013 Eurodac recast Regulation.

²¹⁷ See Article 18(2) of the 2013 Eurodac recast Regulation.

implementation of an automated notification in the procedure of granting citizenship and to include clear and short deadlines for the erasure of data in cases of “advance deletion”²¹⁸.

Eventually, the 2013 Eurodac recast Regulation found a questionable solution that did not create any major changes as it maintained a margin of uncertainty in terms of prompt execution. It established that data should be erased as soon as the Member State of origin becomes aware that the person has acquired the EU citizenship and the Eurodac Central Unit should then inform the other Member States within seventy-two hours²¹⁹. The Eurodac Supervision Coordination Group urged the Member States to inform asylum applicants and migrants of their rights, not only when their fingerprints had been taken, but also in other circumstances – for instance, in cases of acquisition of EU citizenship or of the granting of a national residence permit. It was seen as crucial to make the data subject understand that they had the right to request to access, modify, or erase the data stored in the system. For this purpose, a new provision establishing that the asylum applicant should be given a leaflet containing the information on their subjective rights was inserted, as was information about receiving assistance from the national supervisory authorities and the contact details of the office of the data controller and the national supervisory authorities²²⁰. Furthermore, the leaflet was to be drafted in a language that the person can understand or is reasonably supposed to understand²²¹.

The subsequent Proposal in September 2009 focused on law enforcement and Europol’s access to the system²²² and can be depicted as the most delicate proposal presented by the European Commission in this first batch²²³. This addition was introduced under the cascade approach for which law enforcement authorities were firstly called to compare their national database with those of the other Member States they were given access to under the Prüm Decision²²⁴. Yet, the EDPS raised many concerns because of the changes in the use and purpose

²¹⁸ See the Council of the EU, *Eurodac Coordinated Supervision Group report on advance deletion*, 18885/11, Brussels, 20 December 2011, a manual on best practices was also advanced as a solution to harmonise Member States’ internal rules.

²¹⁹ See Articles 13 of the 2013 Eurodac recast Regulation.

²²⁰ See Article 29(3) of the 2013 Eurodac recast Regulation.

²²¹ *Ibidem*.

²²² It should be noted that the reference to Europol was added in a second step – confront the Council of the EU, *Draft Council Conclusions on access to Eurodac by Member States police and law enforcement authorities*, 8688/1/07, Brussels, 16 May 2007, with Council of the EU, *Draft Council Conclusions on access to Eurodac by Member States police and law enforcement authorities as well as Europol*, 10002, Brussels, 25 May 2007.

²²³ It is interestingly the written question received by the Council of the EU, *Restrictions on the use of Eurodac Data*, 12697/04, Brussels, 23 September 2003, since at that time it firmly rebutted the possibility to access the system for police investigation. Indeed, the access of law enforcement authorities to the Eurodac had been already advanced after the 11-S – see, among others, the Council of the EU, *Policy document concerning access to Eurodac by Member States’ police and law enforcement authorities*, 16982/06, Brussels, 20 December 2006.

²²⁴ Another existing channel for police cooperation mentioned was the Swedish Initiative. The European Commission maintained that these systems were not sufficient since they may not contain data on asylum seekers. It was a hot point later on analysed in Council of the EU, *Opinion of the European Data Protection Supervisor on*

of Eurodac and called for a general debate on law enforcement bodies accessing huge databases²²⁵. Among others, the risk of stigmatisation and of mass surveillance abuse stood out as the searches in the central system were being made without any evidence that the person investigated was supposed to be an asylum applicant. Although the European Commission maintained that law enforcement authorities and Europol's access to the Eurodac presumed an interference with the right to the protection of personal data, it also shared that considering this solution could be more proportionate since it avoided Members States' bilaterally submitted requests spreading migrants' personal data into new areas²²⁶.

In the Proposal, this consultation was restricted twice: first, only those suspected of terrorism and serious crime²²⁷ could be searched for and, second, the requesting authorities should have reasonable grounds to consider that the comparison would contribute to the prevention, detection or investigation of criminal offences. This did not change the EDPS Opinion of 5 September 2012²²⁸ in which the European Commission was strongly criticised because of the lack of an impact assessment that could have evaluated the effects of the proposal on the function creep principle²²⁹. In the end, the 2013 Eurodac Regulation introduced the provision for designated authorities to access the system on a hit/no-hit basis in that it would allow the authorities to see whether the information searched is stored in the system through the so-called National Access Point. If so, and under the supervision of the verification authority, designated authorities could submit a further request to access the Eurodac Central Unit²³⁰. The whole

the Amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], and on the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, 14416/09, Brussels, 16 October 2009, in which it asked for more explanation on the necessity and proportionality of this measure.

²²⁵ See the Council of the EU, 14416/09, Brussels, 16 October 2009, p. 8.

²²⁶ Specifically, a National Contact Point was granted the right to query and access the Central Unit. In case of a match, an administrative cooperation should have been started as the one envisaged under Title VI of the Dublin Regulation.

²²⁷ As defined in the Council Framework Decision of 13 June 2002 on combating terrorism, OJ L 164, 22.6.2002, pp. 3-7, on combating terrorism and the Council Framework Decision 2002/584/JHA.

²²⁸ See the Council of the EU, *Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version) - Opinion of the European Data Protection Supervisor on the amended proposal*, 13420/12, Brussels, 6 September 2012.

²²⁹ See Chapter I.

²³⁰ See Article 7 of the 2013 Eurodac recast Regulation and, among others, the suggestion made by the France delegation, in Council of the EU, *Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of*

procedure should start only after other Member States' databases have been unsuccessfully checked under the Council Decision 2008/615/JHA cooperation mechanism, the VIS has also been searched, and the other existing international mechanisms have been exhausted²³¹.

The results of this long debate flowed into a third Proposal by the European Commission underpinned by Articles 78(2)(e), 87(2)(a) and 88(2)(a) TFEU that finally merged the December 2008 Proposal²³² and the September 2009 Proposal²³³ with the provision of the new agency: eu-LISA²³⁴. Specifically, Articles 87(2)(a) and 88(2)(a) TFEU carried the legacy of the September 2009 Proposal as far as the access of law enforcement authorities and Europol are concerned. Indeed, since December 2012, eu-LISA has been gradually replacing the Management Authority led by the European Commission (DG HOME) and is now fully in charge of its operational management. We will not spend too many words on this subject here as the institutionalisation of the EU operational competence will be examined in the next Chapter. As a result, we will now look at the new 2016 Eurodac recast Regulation.

3.2. The 2016 Eurodac recast Proposal and its amendment

From the very beginning of its implementation, the Eurodac could not achieve its goals because of a lack of cooperation among the Member States. According to the European Commission:

‘[t]he fact that the Eurodac Regulation, as part of the first phase of the [Common European Asylum System], was adopted by unanimous vote in the Council meant that on some points the final text is not sufficiently practice-oriented. This explains why, at present, alignment can prove to be difficult on certain issues (vague deadlines, lack of effective monitoring capacity for the Commission, etc.)’²³⁵.

Regulation (EU) No. [...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No. 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version), 14033/12, Brussels, 30 September 2012.

²³¹ See recitals (32) to (34) of the 2013 Eurodac recast Regulation.

²³² See the Proposal for a Regulation of the European Parliament and of the Council, COM(2008) 825 final, Brussels, 4.5.2016.

²³³ See the Amended proposal for a Regulation of the European Parliament and of the Council, COM(2012) 0254 final - (2008)0242 (COD), Brussels, 4.5.2016.

²³⁴ See the Council of the EU, 10638/12, Brussels, 4 June 2012.

²³⁵ See the Council of the EU, *Commission Staff Working Document accompanying the Proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] - Impact assessment*, 16934/08, Brussels, 9 December 2008, p. 9.

In concrete terms, the European Commission was complaining that Member States were not transmitting, or were delaying the transmission, of information to the²³⁶ Central Unit – now referred to as the Central System²³⁷.

With the new Eurodac recast Regulation adopted on 29 June 2013, a duty to comply within a deadline of seventy-two hours from the taking of fingerprints²³⁸ (though the original Commission Proposal aimed at a stricter deadline of forty-eight hours²³⁹) has been imposed on Member States, or, when the taking of fingerprints is not possible, they have been obliged to transmit the data to the Eurodac Central System as soon as it becomes feasible.

Despite this new provision, Member States failed in submitting asylum applicants' fingerprints during the 2015 humanitarian issue²⁴⁰ which intensified and embittered the debate between Southern/Northern and Eastern/Western Member States on secondary movements²⁴¹. The 2016 Eurodac recast Proposal presented by the European Commission within the frame of its Communication Towards a reform of the Common European Asylum System (CEAS) and enhancing legal avenues to Europe²⁴² marked a turning point for the Eurodac that paved the

²³⁶ With the 2013 Eurodac recast Regulation the Central Unit reference was split between the “Central system” and the “Management Authority” so as to clarify that the former performed automated functionalities, while the latter manual activity. The Management Authority was embodied by the European Commission until another expert body would have been created – see the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person]*, Annex, 16934/08, Brussels, 9 December 2008.

²³⁷ See the Council of the EU, 12928/07, Brussels, 14 September 2007, 11. The European Commission warned that this practice was distorting the Dublin criteria of allocating responsibilities while generating “wrong hits” and “missed hit” and urged Member States to send their data to the Eurodac Central Unit in time.

²³⁸ See Articles 9(1) and 14(2) of the Eurodac recast Regulation.

²³⁹ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person]*, Annex, 16934/08, p. 3, and the Council of the EU, 7649/09, Brussels, 2 April 2009, p. 13.

²⁴⁰ See the Council of the EU, *Commission staff working document on Implementation of the Eurodac Regulation as regards the obligation to take fingerprints, SWD(2015) 150 final*, 9346/15, Brussels, 29 May 2015, in which this failure was indeed endorsed to the no cooperation of the asylum seekers.

²⁴¹ See for example the positions of Belgium, Germany, Finland, France, Hungary, Slovenia, France, and the United Kingdom that insisted in enforcing the wording of Article 2 on the Member States' obligation in registering migrants' fingerprints and also asked for the introduction of sanction in case of no collaboration of the data subject in the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person]*, for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast), 10531/16, Brussels, 8 July 2016, p. 36.

²⁴² See the Communication from the Commission to the European Parliament and the Council, Towards a reform of the common European Asylum system and enhancing legal avenues to Europe, COM(2016) 197 final, Brussels, 6.4.2016. On the Dublin system and its 2016 reform see: Madeline Garlick, “The Dublin System, Solidarity and Individual Rights”, in Vincent Chetail, Philippe de Bruycker and Francesco Maiani, *Reforming the Common European Asylum System*, Leiden, Brill Nijhoff, 2016, pp. 159-194; Bernard Kasperek, “Complementing

way toward the implementation of a new tool for the prevention of, and fight against, irregular migration²⁴³. As a result, a new legal basis was inserted to underpin the Eurodac's goals: Article 79(2)(c) TFEU.

The new Eurodac would aim at identifying irregular migrants residing in the territories of the Member States, or those found while irregularly crossing the external borders to execute their return²⁴⁴. On that occasion, the European Commission advanced the possibility of introducing a new category of biometric data in the Eurodac Central System²⁴⁵ – facial images – as well as some new alphanumeric data²⁴⁶ – i.e., name(s), age, date of birth, nationality, and identity documents²⁴⁷. All the categories of data were supposed to be compared with each other, notwithstanding whether they belonged to international protection seekers or irregular migrants, and the minimum age of capture was lowered to six years old²⁴⁸. Moreover, the data retention period for irregular migrants would be increased to five years – as was agreed in parallel for the SIS II entry ban alert – and irregular migrants to whom a resident permit would be granted

Schengen: The Dublin System and the European Border and Migration Regime”, in Bauder Harald and Matheis Christian, *Migration Policy and Practice. Migration, Diasporas and Citizenship*, London, Palgrave Macmillan, 2016, pp. 59-78.

²⁴³ See the Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast), COM(2016) 272 final, Brussels, 4.5.2016 (2016 Eurodac recast Proposal hereinafter).

²⁴⁴ See Article 1(1)(b) of the 2016 Eurodac recast Proposal.

²⁴⁵ Article 2 of the 2016 Eurodac recast Proposal.

²⁴⁶ On identity documents, Member States asked to have colored copies of passports or identity documents stored so as to facilitate the identification of individual – see the Council of the EU, *Summary Note on the Impact assessment for the Inclusion of Passport Copies (and other scanned documents) to Eurodac*, 7694/17, Brussels, 27 March 2017 and the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] , for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast) - Inclusion of colour copies of passport or ID documents in Eurodac*, 8221/17, Brussels, 12 April 2017.

²⁴⁷ Articles 12, 13 and 14 of the 2016 Eurodac recast Proposal. Member States jumped on this new provision by asking the insertion of a new functionality that would allow the search through alphanumeric data too – see the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) 1077/2011 establishing a European Agency for the operational management of large- scale IT systems in the area of freedom, security and justice (recast)*, 15166/1/16, REV 1, Brussels, 2 December 2016.

²⁴⁸ See Guenter Schumacher, *Fingerprint Recognition for Children*, JRC Technical Reports, Brussels, 2013.

would have their data marked, and not erased, but would not be ‘blocked’ in case of consultations by law enforcement²⁴⁹. Following discussions within the Council of the EU, Member States agreed to insert an *ad hoc* procedure for the taking of minors’ fingerprints, though the provision of using coercive measures as a last resort remedy was maintained²⁵⁰. The obligation of fingerprinting asylum applicants as part of the procedure is marked by a new legal basis that supports the framework of the Eurodac, Article 78(2)(d) TFEU²⁵¹.

On 14 February 2018, the negotiations on the Eurodac were extended so as to include provisions relating to resettlement, though it eventually sank together with the asylum package that has never come to light²⁵². In 2020, the European Commission amended the 2016 Eurodac recast Proposal under the long-awaited Pact on Asylum and Migration presented on 21 September 2020²⁵³. The amended Proposal not only reports the debate on resettlement – which justifies the provision of Article 78(2)(g) TFEU as a further legal basis – but also inserts a new category of individuals whose data will be centrally stored, that is, persons who have entered a

²⁴⁹ See Article 19 (4) and (5) of the 2016 Eurodac recast Proposal. The European Parliament insisted in an equal treatment for EU citizens and permanent residents so that their data should have been deleted as soon as the irregular migrant would have changed his/her status – see the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast) – Preparation for the trilogue*, 9848/18, Brussels, 12 June 2018.

²⁵⁰ See the Council of the EU, 9848/18, Brussels, 12 June 2018. In the case of unaccompanied minors, concretely, the presence of a representative, guardian or trained staff should be present, see recital 25a.

²⁵¹ See the Explanatory Memorandum of the Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of Regulation (EU) XXX/XXX [Regulation on Asylum and Migration Management] and of Regulation (EU) XXX/XXX [Resettlement Regulation], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulations (EU) 2018/1240 and (EU) 2019/818, COM(2020) 614 final, Brussels, 23.9.2020.

²⁵² The corrective allocation mechanism proposed by the European Commission in the new Dublin IV, namely the Proposal for a Regulation of the European Parliament and of the Council, COM(2008) 820 final, 23.9.2009, was a crucial point where Member States could not find an agreement.

²⁵³ Amended proposal for a regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of Regulation (EU) XXX/XXX [Regulation on Asylum and Migration Management] and of Regulation (EU) XXX/XXX [Resettlement Regulation], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulations (EU) 2018/1240 and (EU) 2019/818, COM(2020) 614 final, Brussels, 23.9.2020 (2020 Eurodac amended Proposal). At the time of writing – October 2021 – only the revised Blue Card Directive has been adopted so that there are serious doubts that the Pact will be soon adopted – see the “Droits de l'enfant, Parquet européen, migration et Afghanistan au menu des ministres de la Justice et de l'Intérieur de l'UE”, *Bulletin Quotidien Europe*, No. 12805, 6.10.2010.

Member State following a search and rescue operation²⁵⁴, who have been inserted in the system of allocating responsibilities to examine asylum applications²⁵⁵, or who are beneficiary of temporary protection²⁵⁶. Secondary movements have become a further area to which Eurodac will bring support²⁵⁷, as under the previous Eurodac, secondary movement could not be detected as first-time applicants were not clearly designated as such and only administrative procedures were stored in the system. According to the European Commission, ‘[...] it is necessary to transform the Eurodac system from a database counting applications to a database counting applicants’²⁵⁸. This change will be implemented by linking all the datasets belonging to the same person that are currently dispersed in the system²⁵⁹. Furthermore, the Eurodac will keep the track of migrant movements²⁶⁰: it will record whether an asylum application has been rejected so as to facilitate the return of irregular migrants²⁶¹; it will signal if the return has been executed under a voluntary return and reintegration assistance program²⁶², and it will register if the migrant has been issued a new visa, or has extended an existing one²⁶³. Migrants that represent a threat to internal security will have their data marked in the system²⁶⁴.

It goes without saying that the new amended Proposal²⁶⁵ envisages the integration of the Eurodac into the interoperability framework and, specifically, that its biographic data will be stored in the CIR²⁶⁶. Nevertheless, bilateral forms of interoperability are also envisaged with

²⁵⁴ In which frame, EU agencies cooperate with third countries’ authorities to push back irregular migrants – see “Les pays européens doivent changer d’urgence leurs politiques migratoires, avertit Dunja Mijatović”, *Bulletin Quotidien Europe*, No. 12674, 10.3.2021.

²⁵⁵ See Article 14a of the 2020 Eurodac amended Proposal. It should be noted that under Article 10 of the 2020 Eurodac amended Proposal it is clearly emphasized that the application may now be included in the frame of the screening procedure according to the Proposal for a Regulation of the European Parliament and of the Council introducing a screening of third country nationals at the external borders and amending Regulations (EC) No. 767/2008, (EU) 2017/2226, (EU) 2018/1240 and (EU) 2019/817, COM(2020) 612 final, Brussels, 23.9.2020.

²⁵⁶ “La Présidence française propose d’intégrer dans Eurodac les personnes secourues en mer ainsi que les réfugiés bénéficiant de la protection temporaire”, *Bulletin Quotidien Europe*, No. 12946, 6.5.2022.

²⁵⁷ See Article 1(1)(c) of the 2020 Eurodac amended Proposal.

²⁵⁸ Explanatory Memorandum of the Amended proposal for a Regulation of the European Parliament and of the Council, COM(2020) 614 final, Brussels, 23.9.2020.

²⁵⁹ See Article 4(6) of the 2020 Eurodac amended Proposal.

²⁶⁰ See Article 11 of the 2020 Eurodac amended Proposal.

²⁶¹ See Article 11(2)(dc) of the 2020 Eurodac amended Proposal.

²⁶² See Article 12(z) of the 2020 Eurodac amended Proposal.

²⁶³ See Article 12(u) of the 2020 Eurodac amended Proposal.

²⁶⁴ See Article 12(v) of the 2020 Eurodac amended Proposal.

²⁶⁵ In October 2021, when the European Parliament had not voted on the EU Council’s position yet – see the “Vote on Eurodac planned for mid-November in Committee on Civil Liberties”, *Bulletin Quotidien Europe*, No. 12789, 13.09.2021 –, several NGOs drew the attention of MEPs about: the inclusion of facial images in the Eurodac; the collection of biometric data from children, and the possibility of using coercion to obtain biometric data and the massively expanded scope of the Eurodac – source: “Une trentaine d’ONG s’inquiètent de la future base de données Eurodac sur les demandeurs d’asile”, *Bulletin Quotidien Europe*, No. 12787, 10.9.2021.

²⁶⁶ This implied the additional personal data: place of birth; the type and number of identity or travel document; the three-letter code of the issuing country and validity expiry date. As proposed during the negotiations of the 2016 recast Regulation, the provision of a scanned colored copy of an identity or travel document has been maintained – see Articles 12, 13 and 14 of the 2020 Eurodac amended Proposal.

the ETIAS²⁶⁷ and the VIS²⁶⁸, as part of the terms we analyse in the following paragraphs. Learning from past experiences, it is expected that the 2020 Eurodac amended Proposal will be de-linked from the Pact on Migration and Asylum²⁶⁹ following the EUAA Regulation example so as to be adopted as early as possible²⁷⁰. However, the hasty adoption of laws in sensitive matters that affect vulnerable people's human rights should be discouraged and we call for an accurate and transparent intra-institutional debate on the matter.

4. Visa Information System (VIS)

The project for a VIS gathered force after 11-S following the Conclusions of the European Council of Laeken and Seville when external border management turned out to be vital in the fight against terrorism and illegal migration²⁷¹. At the very beginning, the VIS project would have centralised the information on both short- and long-stay visa holders, yet the latter were finally excluded by the 2008 VIS Regulation for the reasons detailed below. In any case, and despite the opposition of the European Commission, the establishment of a new centralised system should have not substituted the Member States' national databases on visa applicants²⁷².

The VIS represented a jump toward the use of biometric technology for identification purposes²⁷³. The possibility of including biometric identifiers and the establishment of the categories of biometrics that should have been recollected for VIS purposes were endorsed by

²⁶⁷ See Article 8a of the 2020 Eurodac amended Proposal in line with Article 11 of Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, PE/21/2018/REV/1, *OJ L* 236, 19.9.2018, pp. 1-71 (ETIAS Regulation hereinafter), for verification purposes regulated under Articles 20, 22 and 26. The query is carried by the ESP, one of the interoperability components analysed in Chapter V.

²⁶⁸ See the Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), *OJ L* 218, 13.8.2008, pp. 60-81 (VIS Regulation hereinafter). See Article 8c of the 2020 Eurodac amended Proposal for which in order to analyse a visa application, consulate authorities have access to Eurodac as for Articles 9a and 9c of the VIS Regulation, and Article 8d that establishes the interoperability VIS-Eurodac of Article 9a of the VIS Regulation.

²⁶⁹ See the Council of the EU, *Summary of the 38th meeting of the Eurodac Advisory Group, Summary of the 38th meeting of the Eurodac Advisory Group*, 13879/21, Brussels, 12 November 2021.

²⁷⁰ "Les États membres de l'UE évoqueront avec les eurodéputés les difficiles négociations sur les preuves électroniques", *Bulletin Quotidien Europe*, No. 12850, 10.12.2021.

²⁷¹ See the Council of the EU, *Draft Conclusions on the development of the Visa Information System (VIS)*, 9916/03, 2 June 2003, and Council of the EU, "EU Agreement on a VISA Information System", 11306/03, Brussels, 4 September 2003, and the note from the French Delegation confirming it *Development of the Visa System (VIS)*, 14141/04, Brussels, 3 November 2004.

²⁷² Member States are authorised to retrieve data from VIS and insert them in their national files only '[...] in accordance with the purpose of the VIS and in accordance with the relevant legal provisions, including those concerning data protection, and for no longer than necessary in that individual case' according to Article 30 of the VIS Regulation. In this regard, see also the delegations' comments in Council of the EU, *Draft Council Conclusions on the development of the Visa Information System (VIS)*, 5558/04, Brussels, 26 January 2004, p. 10.

²⁷³ See *supra* the difference between verification and identification in the frame of biometric technology.

the political input of the EU Council²⁷⁴, that finally decided to build the new system in two phases: in the first stage, the VIS would have processed only alphanumeric data and photographs; in the latter phase, biometric identifiers should also have been added²⁷⁵. As with the Eurodac, the VIS was equipped with an AFIS in order to launch biometric searches. However, in this case, biometrics are part of the individual's identity file, in order to allow the system to identify a subject by retrieving the corresponding alphanumeric data. Indeed, in cases of a match between the data inserted in the system and the one stored therein, the VIS will enable the retrieval of the entire identity file containing the information of the person searched for.

Since the VIS and the SIS II projects were presented at the same time, the European Commission proposed to design and implement their architecture, location, and the communication infrastructure in a synergistic manner²⁷⁶. Furthermore, and despite the objections raised by some delegations at the beginning²⁷⁷, VIS users should have been able to access the SIS II via the central VIS before issuing a visa²⁷⁸; while police, immigration, and borders authorities would have been authorised to consult the VIS through the SIS II in order to accomplish their tasks²⁷⁹.

4.1. The VIS Regulation

The first VIS proposal was presented by the European Commission in 2004 in order to allow the inclusion of the VIS in the Community budget and to execute part of it²⁸⁰. This proposal was presented on the basis of the sole Article 66 of the 2002 TEC and assumed that the Decision '[...] concern[ed] the development of a system for cooperation via the exchange of visa data

²⁷⁴ At the beginning, also the iris scanning was contemplated – see the Council of the EU, 11306/03, Brussels, 4 September 2003.

²⁷⁵ See the Council of the EU, 14776/03, Brussels, 13 November 2003.

²⁷⁶ See the Council of the EU, 16106/03, Brussels, 15 December 2003. The VIS indeed was located in Strasbourg with a back-up central VIS in Sankt Johann im Pongau, see Article 27 of the VIS Regulation.

²⁷⁷ See, among others, Council of the EU, *Development of the Schengen Information System II and possible synergies with a future Visa Information System (VIS)*, 6253/04, Brussels, 13 February 2004.

²⁷⁸ See Article 101 (2) of the Convention implementing the Schengen Agreement for which:

'If a search brings to light an alert for an object which has been found, the authority which matched the two items of data shall contact the authority which issued the alert in order to agree on the measures to be taken. For this purpose, personal data may also be communicated in accordance with this Convention. The measures to be taken by the Contracting Party which found the object must be in accordance with its national law'.

²⁷⁹ See the Spanish Delegation comment here Council of the EU, *Draft Council Conclusions on the development of the VISA Information System (VIS) Comment to the document 14776/1/03 VISA 187 COMIX 691 REV 1*, 5335/04, Brussels, 15 January 2004.

²⁸⁰ See the Council of the EU, *Proposal for a Council Decision establishing the Visa Information System (VIS)*, 6373/04, Brussels, 16 February 2004.

between Member States, "which have abolished checks at their internal borders" and participate "in the system of free movement without checks at internal borders"²⁸¹.

Therefore, the European Commission foresaw that the Decision should have regulated the exchange of visa data among the relevant departments of the Member States responsible for issuing visas and implementing border checks in the areas covered by Title IV of the 2002 TEC, as well as between those departments and the European Commission. As a consequence, in the European Commission's opinion, the new measure did not concern substantial revision of visa policies. Remarkably, the cooperation among administrations would have been enhanced by the creation of a VISION Network to enable consultations among the central authorities of the VIS and the consulates as well²⁸². Since this Regulation did not claim to regulate the functioning of the VIS, but was only presented for funding purposes, the European Commission announced the presentation of a further legal text where the characteristics of the system were elaborated upon.

In its second Proposal, the European Commission presented the Regulation concerning the VIS and the exchange of data between Member States regarding immigrants on short stays²⁸³. The Proposal aimed at giving the European Commission the mandate for the setting up and maintaining of the VIS²⁸⁴. As announced, its range of application was limited to short-stay visas only, since the Member States' policies on long-stay visas were not considered to be included under Article 63(3)(a) of the 2002 TEC. According to this norm, the European Commission was empowered to adopt measures on 'conditions of entry and residence, and standards on procedures for the issue by Member States of long-term visas and residence permits, including those for the purpose of family reunion'. Yet, following the guidelines of the Council Legal Service, the legal framework of the VIS Proposal was enhanced by the presence of Article 62(2)(b)(ii) of the 2002 TEC, as the consultation of the VIS was perceived as an indispensable step for the issuing of short-stay visas – or Schengen visa²⁸⁵ – and, specifically, it would have been part of '[...] the procedures and conditions for issuing visas by Member States'²⁸⁶. In the

²⁸¹ *Ibid.*, p. 5.

²⁸² See Article 16 of the VIS Regulation, that seemed from Article 17(2) of the Convention implementing the Schengen Agreement.

²⁸³ See the Council of the EU, *Proposal for a Regulation of the European Parliament and the Council concerning the Visa Information System (VIS) and the exchanging of data between the Member States on short-stay visa*, 5093/05, Brussels, 4 January 2004. Nevertheless, many delegations complained the lack of reference to the long stay visa and insisted for its insertion too – see the Council of the EU, *Draft Regulation of the European Parliament and the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-visa*, 6921/05, Brussels, 16 March 2005, p. 12. The document is partially accessible to the public, so it is not possible to distinguish which delegations concretely intervened.

²⁸⁴ See recital (3) in the Council of the EU, 5093/05, Brussels, 4 January 2004.

²⁸⁵ According to Articles 9 to 17 of the Convention implementing the Schengen Agreement.

²⁸⁶ See Article 1 of the VIS Regulation.

Council Legal Service's point of view, Article 66 of the 2002 TEC would have justified the '[...] structure and functionalities of the VIS, including the provisions on data protection, as well as for the provisions allowing the exchange of data between the competent visa authorities by means of access to the system'²⁸⁷, which is surprising, provided that data protection was not even mentioned under Article 66 of the 2002 TEC and the EU had no express competence on it. Conversely, Article 62(2)(b)(ii) of the 2002 TEC would have addressed the procedure covered under the second chapter of the proposed Regulation and, concretely, the issuing of visas. The two legal bases were perceived as indispensable to combat the phenomenon of "visa shopping" and to facilitate the development of a common visa policy. Therefore, the Council Legal Service adopted a function-oriented approach to legitimise the choice of the correct legal basis according to the purposes for which the system was consulted or accessed. Provided that Article 66 of the 2002 TEC shifted from unanimity to a qualified majority on 1 January 2004²⁸⁸ the two legal bases were found to be mutually compatible and the codecision procedure prevailed.

However, this position led to a further analysis on the use of the VIS data by other authorities, namely border authorities, immigration authorities, asylum authorities and law enforcement authorities. Indeed, apart from its contribution to the administration of a common visa policy, the VIS Regulation was enriched with a series of different purposes that aimed to:

- prevent internal security threats;
- stop the submission of numerous visa applications in different Member States by one individual, also known as 'visa shopping';
- detect fraud during checks at the external borders as well as within the territories of the Member States;
- identify third country nationals for the purposes of return²⁸⁹, and
- evaluate an asylum application according to the Dublin system²⁹⁰.

Thus, access to the system was granted to authorities other than visa officials, which led to the Council Legal Service and the European Commission holding two opposed positions: while

²⁸⁷ See the Council of the EU, 6683/05, Brussels, 23 February 2005, p. 5.

²⁸⁸ See the declaration annexed to the Treaty of Nice amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, *OJ C* 80, 10.3.2001, pp. 1-87, for which: 'From 1 May 2004, the Council shall act by a qualified majority, on a proposal from the Commission and after consulting the European Parliament, in order to adopt the measures referred to in Article 66 of the Treaty establishing the European Community'.

²⁸⁹ During the negotiations it was stressed that the purpose of VIS is to identify the migrant and not to return him/her, though identification would be prodromic to it – see the Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between the Member States on short-stay visa*, 12190/06, Brussels, 7 September 2006.

²⁹⁰ See Article 2 of the VIS Regulation.

the former asked for the insertion of the relevant legal bases the policies of which the VIS would have supported, the latter considered that a unique legislative text underpinned by Article 66 of the 2002 TEC was sufficient to account for the different usages of the VIS by border, immigration and asylum authorities²⁹¹. In its argument, the Council Legal Service recalled that the data stored in the VIS should have been collected for a specific, explicit, and legitimate purpose and that any further processing must be compatible with the former purpose. Therefore, the aim of the measure should have been specified in order to guarantee access to the data for authorities other than those involved with the processing of visas. With regard to border authorities and immigration authorities, the Council Legal Service recognised that these authorities were given access to the system to verify the identity of third country nationals and, as with visa authorities, they belonged to the administrative departments of the Member States. Nevertheless, the inclusion of their activity under Article 66 of the 2002 TEC was questioned. The Council Legal Service recalled that in the opinion on the Council Regulation (EC) No 871/2004 on the introduction of new functions for SIS II, including the fight against terrorism, Article 66 of the 2002 TEC was considered to be a sufficient legal basis, while Articles 62 and 63 of the 2002 TEC were discarded as it was assumed that SIS II neither aimed at controlling external borders nor sought to regulate the entry and residence of third country nationals in the Schengen area. Interestingly, the Council Legal Service justified its position maintaining that the common visa policy was not an aim pursued by the Convention implementing the Schengen Agreement, but rather that it integrated one of the elements of the common immigration policy. Specifically, the establishment of a common legal framework on the conditions of entry to the Schengen area should have been read in light of the general objective of abolishing internal border controls and promoting the freedom of movement. In its words:

‘Even if those provisions are a distinct but inseparable element, they may be considered as subordinate to the general objective’²⁹².

As a result, the access of visa authorities to the SIS II data should have not been inserted in the SIS II legal framework. Nevertheless, the Council Legal Service found treating the access of border and immigration authorities to the VIS as subordinated to the visa policy to be the wrong approach. On the contrary, consultation of the VIS was vital if the authorities were to comply with the broader common immigration policy. As a consequence, and unlike the SIS II, Articles 62(2)(a) and 63(3)(b) of the 2002 TEC should have been inserted into the legal framework of the VIS. As for asylum authorities, access to the VIS was justified in light of the

²⁹¹ See Article 67 of the 1997 TEC.

²⁹² See the Council of the EU, 6683/05, Brussels, 23 February 2005, p. 5.

Dublin system and, concretely, in order to determine which Member State was responsible for examining an asylum application. In this sense, Article 63(1)(a) of the 2002 TEC was clearly the sole legal basis valid for regulating access to the VIS by asylum authorities²⁹³. Finally, the Council Legal Service also analysed the access of law enforcement authorities to the VIS. In this area, it was clear that Article 66 of the 2002 TEC could have not been applied to the third pillar measure since its scope remained limited to the provisions of the 1997 TEC only. A separate Decision should have been adopted on the basis of Article 29 of the 2002 TEU. All in all, the Council Legal Service stated that Articles 62(2)(a), 63(3)(b), and 63(1)(a) of the 2002 TEC should have been inserted in the European Commission Proposal so as to legitimise access to the system by border, immigration, and asylum authorities. Steps should have been taken to ensure the compatibility of the law-making procedures, though these new provisions were deemed not to undermine the balance among the legal bases. All in all, the codecision procedure was confirmed to be the correct path to follow.

For its part, the European Commission contested the position assumed by the Council Legal Service and stressed that Article 66 of the 2002 TEC constituted a sufficient legal basis for the adoption of the proposed VIS Regulation while including the consultation made by border guards, migration, and asylum authorities²⁹⁴. It also underlined that the splitting of the proposal would have hindered the decision-making procedure.

As a last resort, the Council Legal Service called for the presentation of a new proposal referencing Articles 16 to 19 on border guards, immigration authorities, and asylum authorities underpinned by Articles 62(2)(a), 63(3)(b), and 63(1)(a) of the 2002 TEC. According to the Council Legal Service, these purposes were not contained in Article 62(2)(b)(ii) of the 2002 TEC and a “bridge clause” would have been sufficient to establish cross-references among the legislative texts. However, the European Commission maintained that by inserting the relevant consequential amendments there would be no need to adopt a number of new texts. In the end, the basis of the VIS Regulation was found in Article 62(2)(b)(ii) and Article 66 of the 2002 TEC, and the European Commission had defeated the Member States’ positions for the time being. It is interesting to note that by only binding the Member States and the European Commission’s administrations, it was doubtful whether the information processed through the VIS could have been exchanged with third parties in light of the cooperation principle set forth

²⁹³ See the C-271/94, *European Parliament v Council of the European Union*, 26 March 1996, EU:C:1996:133.

²⁹⁴ See the Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-visas Chapter III (Articles 16 to 19) and Chapter VII (Articles 36 to 41) – Second reading*, 12663/05, Brussels, 7 November 2005.

under Article 66 of the 2002 TEC²⁹⁵. However, the opportunity to forward data to third countries in order to prove the identity of third country nationals turned out to be a very attractive solution in combatting irregular migration and Member State agreed to “open” the frontlines of their database as we will further analyse in Chapter VI²⁹⁶.

The vertical cooperation between Member States and the European Commission is reflected by the insertion into the VIS Regulation of provisions on shared responsibilities on different layers. While the European Commission was depicted as responsible for the central infrastructure, each Member State had to develop a national infrastructure²⁹⁷. Specifically, Member States would have been responsible for their National System and for the interconnection of such systems with the National Interface²⁹⁸. However, the National Interface, together with the Central VIS, would have been assigned to the European Commission²⁹⁹ under the following terms:

‘The activities of the Commission are limited to the setting-up and maintenance of the Central Visa Information System, the National Interfaced and the communication infrastructure between the Central VIS and the National Interfaces, whereas the competence for its National System remains by each Member State’³⁰⁰.

Furthermore, while the European Commission was responsible for the security of the Central VIS, the Member States supported the vast majority of the communication infrastructure, access to the system by authorised staff, and the security measures concerning the VIS, with the help of a Management Authority established after the transitional period. The Management Authority was in charge of the operational management of the VIS after an undefined transitional period, and it should have developed the ‘[...] tasks necessary to keep the VIS functioning twenty-four hours a day, seven days a week in accordance with this Regulation, in particular the maintenance work and technical developments necessary to ensure that the system functions at a satisfactory level of operational quality, in particular as regards the time required for interrogation of the central database by consular posts, which should be as short as possible’³⁰¹. As is further analysed in Chapter IV, the Management Authority later evolved into eu-LISA.

²⁹⁵ See the Council of the EU, *Draft Conclusions on the development of the Visa Information System (VIS)*, 6010/04, Brussels, 9 February 2004, p. 2.

²⁹⁶ See Article 31 of the VIS Regulation and our analysis made in Chapter VI.

²⁹⁷ See Article 2 of the Council of the EU, 6373/04, Brussels, 16 February 2004.

²⁹⁸ See Article 24 of the Council of the EU, 5093/05, Brussels, 4 January 2004.

²⁹⁹ See the Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-visas*, 8983/05, Brussels, 8 June 2005.

³⁰⁰ See the Council of the EU, 5093/05, Brussels, 4 January 2004, p. 6.

³⁰¹ See Article 26(8) of the VIS Regulation.

As a result, the European Commission and the Member States are in charge of the Central and National systems respectively, including: the lawfulness of processing; the accuracy of data; any unauthorised access; the control of data media, and the recording of the entry, access to, and the transmission and transfer of data³⁰². However, Member States alone supervise the responsibility for the use of data – i.e., the lawfulness of processing – and they are liable for the damages caused by any unlawful processing committed by their national authorities³⁰³. Indeed, the European Commission was clearly pointed out as a mere “mediator” of data on behalf of the Member States and, as a consequence, it was intentionally not depicted as the data controller³⁰⁴. Besides, although record-keeping was presented as a shared duty/responsibility between the Member States and the Management Authority, the former maintained the monopoly on the records of the national authorities that were able to enter data in the National system³⁰⁵.

In addition to this, a “self-monitoring” option was introduced so that Member States themselves could monitor the lawfulness of the access granted to the data stored in the VIS. The EDPS underlined that the self-monitoring activity should have included self-auditing compliances in order to check that any usage of the data entered into the VIS complied with the data protection requirements³⁰⁶. Following the same logic, Member States should have, according to their national law, established the relevant sanctions or penalties³⁰⁷ in case the system was misused³⁰⁸. This provision was inserted on the basis of the CJEU case-law on the provision of effective, proportionate, and dissuasive measures within criminal law in the EU environmental policy³⁰⁹ since these measures were considered to be necessary to achieve a common policy³¹⁰. However, the provision of a criminal law disposition in an ex-first-pillar instrument raised concerns among the delegations that highlighted the need for involvement by the Coordinating Committee in the area of police and judicial cooperation in criminal matters (CATS) in order to assess if any steps being taken were appropriate.

³⁰² See Articles 26 and 28 of the VIS Regulation.

³⁰³ See Article 33 of the VIS Regulation.

³⁰⁴ See Article 23 of the Council of the EU, 5093/05, 4 January 2004.

³⁰⁵ See Article 34 of the VIS Regulation.

³⁰⁶ See the Council of the EU, *Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences*, 7599/06, Brussels, 20 March 2006.

³⁰⁷ See Article 26 of the VIS Regulation.

³⁰⁸ See Articles 35 and 36 of the VIS Regulation.

³⁰⁹ C-176/03, *Commission of the European Communities v Council of the European Union*, 13 September 2005, EU:C:2005:542.

³¹⁰ See the comments from The Netherlands delegation Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas*, 16225/06, Brussels, 5 December 2006.

In the end, National Supervisory Authorities and the EDPS were responsible for monitoring the Member States and the European Commission's lawfulness in processing personal data according to the DPD and the DPREC³¹¹. Also, Member States' national supervisory authorities were asked to cooperate in order to correct and erase the data, where necessary. Indeed, the Member State that input the data maintained their managerial responsibility and should have been consulted in case of further modifications³¹².

As for the categories of data stored in the VIS, alphanumeric and biometrics were both considered³¹³. This implied that the visa stickers contained biometrics³¹⁴ and that the VIS was furnished with a shared biometric matching system where the biometrics templates were stored. Fingerprints – ten prints, except in the case of children – and photographs were the two categories of biometric data processed in the VIS, but the latter are not used for the purposes of biometric identification because of their generally poor quality, which increases the risk of false positives and false negatives³¹⁵.

Generally speaking, as for the Member States' approach to the data protection requirements it should be appreciated that, unlike the negotiations on the Eurodac, Member States demonstrated that they had acquired a better understanding of EU data protection legislation and its applicability in the AFSJ since delegations did not question the application of the DPD to the VIS. This did not prevent attempts to restrict the guarantees set forth in the new Regulation and Member States repeatedly asked to store more information in the VIS³¹⁶. Among these requests, they suggested inserting new data on travel medical insurance and on

³¹¹ See Articles 34 and 35 in the Council of the EU, 5093/05, Brussels, 4 January 2004.

³¹² See Article 32 in the Council of the EU, 5093/05, Brussels, 4 January 2004.

³¹³ See Article 5 of the VIS Regulation. Note that different categories of data are entered depending on the different stage of the proceeding: to lodge the application (Article 9); when the visa is issued (Article 10); when the visa is refused (Article 12); when the visa is annulled or revoked (Article 13), and when the visa has been extended (Article 14).

³¹⁴ See the Council Regulation (EC) No 1683/95 of 29 May 1995 laying down a uniform format for visas, *OJ L* 164, 14.7.1995, pp. 1-4, current Regulation (EU) 2017/1370 of the European Parliament and of the Council of 4 July 2017 amending Council Regulation (EC) No 1683/95 laying down a uniform format for visas, *OJ L* 198, 28.7.2017, pp. 24-28.

³¹⁵ See Article 5(1)(b) and (c) of the VIS Regulation.

³¹⁶ Another example can be consulted in the Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States and short-stay visa*, 8325/06, Brussels, 12 April 2006, where Member States attempted to restrict the right to information of data subject under the conditionality of a request or in case it would have been estimated as appropriate, while excluding its recognition in cases of national interest. The European Commission, on the contrary stressed that the principle of transparency and data protection asked for the provision of information always. Furthermore, it opposed to the request of deleting the provision on "remedies" by stressing that the reference to a court should have been maintained by virtue of Article 22 of DPD.

the person issuing the invitation, such as the date of birth, phone number, e-mail address, gender, place or state of birth, and national identity card number³¹⁷.

A huge debate was started by the German delegation, that proposed the insertion of a new Article 11a sanctioning third country nationals in case of visa “misuse”³¹⁸. According to the proposed Article, the identity file stored in the VIS should have highlighted visa holders overstaying the duration of their visa in the territories of Member States in cases of unlawful employment, upon the receipt of a refusal of an asylum application, and for any other reason justifying the refusal of the visa. Yet, the creation of a “sponsored database” raised some complications in the European Parliament that called for a more transparent debate³¹⁹. The EDPS highlighted how the problem of sponsors could have been easily tackled at national level in accordance with the subsidiarity principle³²⁰. It is clear that this provision would have jeopardised visa applicants, especially in light of future applications as it could restrict their access to the Schengen area³²¹. Finally, the European Parliament proposed to delete the proposed Article until the adoption of the Visa Code and invited the European Commission to provide the co-legislators with further reports³²².

Another important discussion concerned the age limit for the collection of data from children³²³. During the negotiations, the European Commission advanced the possibility of capturing fingerprints from five-year-old children to perform one-to-one searches. Also, the presence of a biometric expert was suggested, taking into account that children’s samples change quickly in a short period of time. However, the capture of children’s facial images was discarded because of the significant changes they undergo until the age of eleven³²⁴. For all categories of applicants, the period of storage was set at a maximum of five years – although

³¹⁷ See the Council of the EU, *Draft Regulation of the European Parliament and the Council Concerning the Visa Information System (VIS) and the exchange of data between Member States on short-visa*, 11090/05, Brussels, 27 July 2005.

³¹⁸ See Article 11a in the Council of the EU, 8325/06, Brussels, 12 April 2006, p. 33.

³¹⁹ See the Letter from the LIBE Committee in the Council of the EU, *Draft Regulation of the European Parliament and the Council concerning the Visa Information System (VIS) and the exchange of data between the Member States on short-stay visas*, 9130/06, Brussels, 8 May 2006.

³²⁰ See the EDPS in Council of the EU, *Draft Regulation of the European Parliament and the Council concerning the VISA Information System (VIS) and the exchange of data between the Member States on short-stay visas*, 10734/20, Brussels, 4 June 2006.

³²¹ *Ibid.*, p. 2.

³²² See the Council of the EU, *Draft Regulation of the European Parliament and the Council concerning the Visa Information System (VIS) and the exchanging of data between the Member States on short-stay visa*, 16229/06, Brussels, 6 December 2006, p. 3.

³²³ See the Council of the EU, *Exemptions from the fingerprinting requirements in the Visa Information System (VIS)*, 12699/05, Brussels, 28 September 2005.

³²⁴ See the Council of the EU, *Setting of minimum age for recoding and storing facial images and fingerprints on the chip of a passport or residence and in the Visa Information System*, 9403/06, Brussels, 23 May 2006.

the delegations asked for a longer period³²⁵ – after which the data was to be deleted in an automated manner³²⁶. Moreover, the application files stored in the VIS was to be linked to one another so as to identify the applicant or a group of applicants travelling together³²⁷.

Apart from the competent consular authorities and central visa authorities responsible for examining a visa request, the VIS can also be accessed by other authorities through a biometric verification recognition procedure or, subsidiarily, through a biometric search. These authorities include border guards who verify the identity of the visa applicant and immigration authorities in charge of identifying third country nationals and controlling the fulfilment of the conditions of entry, stay, or residence³²⁸. Along the same lines, asylum authorities were allowed to launch biometric searches using fingerprints in the VIS to determine which Member State was in charge of analysing the asylum application and also for examining the asylum application itself³²⁹. This last provision was strongly supported by the Member States and represented the VIS shifting into Article 63(1)(a) of the 2002 TEC on the individualisation of the Member State responsible for an asylum application. In sum, as different categories of migrants could not be identified through Eurodac, Member States were allowed to consult the VIS³³⁰.

One of the most delicate areas regarding the different categories of authorities with access to the VIS was the consultation of the system for the realisation of border checks. The VIS Regulation established that biometric verification at the borders should be conducted with the use of the visa sticker and the fingerprints³³¹. However, during the negotiations some delegations feared that the use of biometrics at the borders would slow down crossing of, and transit from, the border and asked for a more flexible approach – i.e., they believed that a search using the visa sticker should have been sufficient³³² – and that different measures should be employed depending on the type of border in question – land, sea, or air³³³. On the other hand, other States, firmly supported the insertion of systematic biometric checks to avoid “border

³²⁵ See the Council of the EU, Council of the EU, 8983/05, Brussels, 8 June 2005, p. 35.

³²⁶ See Article 23 of the VIS Regulation.

³²⁷ See Article 5(3) and (4) of the Council of the EU, 5093/05, Brussels, 4 January 2004.

³²⁸ See articles 18-20 of the VIS Regulation.

³²⁹ See articles 21 and 22 of the of the VIS Regulation.

³³⁰ See the Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-visa Chapter III (Articles 16 to 19) and Chapter VII (Articles 36 to 41) – Second reading*, 13663/05, Brussels, 7 November 2005.

³³¹ Article 18(1) of the VIS Regulation.

³³² See the position of Poland in the Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas*, 6438/07, Brussels, 15 February 2007.

³³³ See the Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas*, 8198/07, Brussels, 2 April 2007.

shopping” and suggested the insertion of an exceptional clause to authorise the suspension of biometric checks only for compelling reasons³³⁴. This option was the one favoured by the VIS Regulation team, yet a compromise was found by providing Member States with a transitional period in which searches could be undertaken using only the visa stickers³³⁵.

The consultation of the VIS at the external borders, and especially the undertaking of biometric searches, demanded an amendment to the Common Consular Instructions³³⁶ and to the Schengen Borders Code³³⁷ in order to harmonise the consultation of the VIS during the first-line border controls³³⁸. The Regulation complements the VIS Regulation, yet it is based on Article 62(2)(a) of the 2002 TEC stating that the European Community could adopt measures related to checks at external borders. The discussions raised on this occasion put into evidence the difficult balance between the guarantee of fast and smooth controls for travellers and the need to enhance security: while the former would have opted for the use of the visa sticker alone as a general rule, the latter sought the imposition of the systematic consultation of the VIS through the biometric verification procedure³³⁹. The European Parliament Rapporteur’s comment is significant in this sense, while affirming that:

‘[...] no one knows how many visas have been forged in the past. Taking fingerprints is a very time-consuming process and causes long queues at borders for EU and non-EU citizens alike (in this regard, he particular cited the case of the border between Slovenia and Croatia on public holidays). There is a need to balance convenience and security. The European Union should not introduce a new Berlin Wall, but should continue to be citizen- and tourist-friendly’³⁴⁰.

³³⁴ See the position of France in Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas – Article 16*, 6531/07, Brussels, 19 February 2007.

³³⁵ See Article 18 of the VIS Regulation that establishes a three-year transitional period, that could be reduced in case of air borders.

³³⁶ See the Common Consular Instructions on visas for the diplomatic missions and consular posts, *OJ C* 313, 16.12.2002, pp. 1-96.

³³⁷ At that moment, Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code), *OJ L* 105, 13.4.2006, pp. 1-32.

³³⁸ See the Regulation (EC) No 81/2009 of the European Parliament and of the Council of 14 January 2009 amending Regulation (EC) No 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Borders Code, *OJ L* 35, 4.2.2009, pp. 56-58.

³³⁹ See the Council of the EU, *Draft Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of Visa Information system (VIS) under the Schengen Border Code*, 9401/08, Brussels, 16 May 2008.

³⁴⁰ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Borders Code – Outcome of the European Parliament's first reading (Brussels, 1 to 4 September 2008)*, 12704/08, Brussels, 15 September 2008, which remains more an objective of the Union than a will of the Member States, as we see in the news “L’argent européen n’est pas destiné à financer des ‘murs’ anti-migrants aux frontières extérieures de l’UE, souligne la Commission”, *Bulletin Quotidien Europe*, No. 12808, 9.10.2021.

According to the adopted amendments, consultation of the VIS shall make use of both visa stickers and fingerprints, but only on a random basis or in cases where there are doubts regarding the identity of the third country national or the authenticity of the visa. Otherwise, searches via visa sticker checks shall be considered as the general rule³⁴¹. However, this option was only valid for a transitional period of three years, after which the European Commission was to present further amendments in order to give priority to systematic biometric checks³⁴². Along the same lines, the European Commission should have considered the possibility of improving the infrastructure at the border crossing points³⁴³.

4.2. The access of law enforcement authorities and of Europol to the VIS: The VIS LEA Decision

A “bridging Decision” was adopted in order to grant law enforcement authorities and Europol access to the VIS for the purposes of preventing, detecting and investigating terrorist offences under the provisions of the Title VI of the TEU³⁴⁴. This Decision was mirrored in the VIS Regulation through a “bridging disposition” that caused widespread discussion in light of the European Parliament’s position of insisting on the insertion of major guarantees. Specifically, the European Parliament sought to inserting the following dispositions:

- the provisions of Central Access Point(s) in the Member States;

³⁴¹ The other way around would have consisted in implementing systematic checks with both visa stickers and fingerprints and visa sticker only in exceptional cases – see the LIBE Committee comments in the Council of the EU, 9401/08, Brussels, 16 May 2008.

³⁴² See Article 1(1)(ae) of the Regulation (EC) No 81/2009 of the European Parliament and of the Council of 14 January 2009 amending Regulation (EC) No 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Borders Code, OJ L 35, 4.2.2009, pp. 56-58, that followed the Germany suggestions in Council of the EU, *Draft Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of Visa Information system (VIS) under the Schengen Border Code*, 10109/08, Brussels, 29 May 2008.

³⁴³ See the Council of the EU, *Draft Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of Visa Information system (VIS) under the Schengen Border Code – Draft statement from the Council meeting*, 13643/08, Brussels, 1 October 2008. The evaluation was conducted under Article 50(4) of the Council of the EU, *VIS Regulation in the Commission Staff Working Document Evaluation of the implementation of Regulation (EC) No 767/2008 of the European Parliament and Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) / REFIT Evaluation Accompanying the document Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the Visa Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation*, 13530/16 ADD 2, Brussels, 21 October 2016.

³⁴⁴ See the Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218, 13.8.2008, pp. 129-136 (VIS LEA Decision hereinafter). At the very beginning, the Proposal was justified in the light of the possibility that the visa could have been falsified to enter the Schengen area – see the Council of the EU, *Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences*, 15142/05, Brussels, 20 November 2005, p. 4.

- the implementation of prior checks with regard to any requests to access the system;
- the possibility to access the system on a case-by-case basis, and
- the prior adoption of the DPFD³⁴⁵.

The Proposal was underpinned by the third pillar framework of Articles 30(1)(b) and 34(2)(c) of the 2002 TEU. The European Parliament stressed that the access of authorities and bodies to the VIS should have been clearly limited so as to not void the nature of the system:

‘The [European Parliament] is of the opinion that this will not lead to a waste of time or resources and states that, as the VIS is not a criminal database, checking the VIS should be a second line measure anyway’³⁴⁶.

For its part, the EDPS added that any ‘[r]outine access would indeed represent a serious violation of the principle of purpose limitation. It would entail a disproportionate intrusion in the privacy of travelers who agreed to their data being processed in order to obtain a visa, and expect their data to be collected, consulted and transmitted, only for that purpose’³⁴⁷. Following the negotiations, the access of law enforcement authorities was limited to specific purposes for the prevention, detection, and investigation of terrorist offences and other serious criminal offences³⁴⁸; the following issues should be considered and be respected in order to access the information³⁴⁹: first, accessing the VIS must be necessary for a specific case and, second, accessing the VIS data must be part of reasonable steps in the prevention, detection, or investigation of criminal offences.

Nevertheless, the lack of a harmonised measure regarding the protection of personal data when used by law enforcement authorities raised further issues, especially within the European Parliament, that in a voting session affirmed that ‘[...] differences between Member States concerning data protection could be too wide. Furthermore, there are also big differences in

³⁴⁵ See, among others, the Council of the EU, *Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences*, 14196/06, Brussels, 19 October 2006, p. 3.

³⁴⁶ See the Council of the EU, *Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences*, 14196/2/06, Brussels, 22 December 2006, p. 2.

³⁴⁷ See the Council of the EU, *a) Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-visa b) Council Decision concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member State and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences*, 8540/07, Brussels, 18 April 2007, p. 4.

³⁴⁸ See Article 1 of the VIS LEA Decision.

³⁴⁹ See Article 5(1) for the national designated authorities and Article 7(1) for Europol in the VIS LEA Decision.

estimations on costs³⁵⁰. The EDPS specified that the application of the data protection norms set forth in the Decision should have been regarded as *lex specialis* with regard to the DPFD³⁵¹. In case the legislative framework on data protection was not applicable to the intelligence authorities, Member States should have taken appropriate measures.

The VIS LEA Decision should have become enforceable together with the VIS Regulation so that the system could have been fully operational from the very beginning. For this purpose, a Council Implementing Decision should have been adopted³⁵². However, the Council Decision (EU) No 2013/392/EU³⁵³ was invalidated by the CJEU due to the lack of consultation with the European Parliament, according to Article 39(1) of the former TEU³⁵⁴. On this occasion, the European Parliament assumed that the act was implicitly underpinned by Article 34(2)(c) of the 2002 TEU, though the act broadly referred to the TFEU and the VIS LEA Decision. That legal basis had been repealed by the 2007 Lisbon Treaty, and the European Parliament alleged that the Council could not adopt such a new measure on that ground³⁵⁵. The Council, for its part, maintained that the Decision had been adopted based on Article 18(2) of the VIS LEA Decision³⁵⁶ read in conjunction with Article 9 of Protocol No 36 to the 2007 Lisbon Treaty on the transitional provisions³⁵⁷. In the end, the CJEU rejected the European Parliament's allegations and highlighted that the Council Decision did not refer to Article 34(2)(c) of the 2002 TEU. The CJEU also analysed the validity of such a "secondary legal basis" that excluded

³⁵⁰ See the Council of the EU, *Proposal of a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-visa – Outcome of the European Parliament's first reading (Brussels, 6 to 7 June 2007)*, 9753/07, Brussels, 19 June 2007, p. 4.

³⁵¹ See Chapter I.

³⁵² See the Council of the EU, *Council Decision fixing the date of effect of Decision 2008/633/JHA concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences*, 11431/13, Brussels, 17 July 2013.

³⁵³ Council Decision 2013/392/EU of 22 July 2013 fixing the date of effect of Decision 2008/633/JHA concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, *OJ L* 198, 23.7.2013, pp. 45-46.

³⁵⁴ According to which: 'The Council shall consult the European Parliament before adopting any measure referred to in Article 34(2)(b), (c) and (d). The European Parliament shall deliver its opinion within a time limit that shall not be less than three months. In the absence of an opinion within that time limit, the Council may act' – see the C-540/13, *European Parliament v Council of the European Union*, 16 April 2015, EU:C:2015:224.

³⁵⁵ Article 34(2)(c) of the VIS Regulation sets forth that:

'The Council shall take measures and promote cooperation, using the appropriate form and procedures as set out in this Title, contributing to the pursuit of the objectives of the Union. To that end, acting unanimously on the initiative of any Member State or of the Commission, the Council may: [...] adopt decisions for any other purpose consistent with the objectives of this Title, excluding any approximation of the laws and regulations of the Member States. These decisions shall be binding and shall not entail direct effect; the Council, acting by a qualified majority, shall adopt measures necessary to implement those decisions at the level of the Union [...].'

³⁵⁶ 'This Decision shall take effect from a date to be determined by the Council once the Commission has informed the Council that Regulation (EC) No 767/2008 has entered into force and is fully applicable'.

³⁵⁷ Protocol No 36.

the European Parliament from the law-making procedure and affirmed that only the Treaties could have modified such a procedure. As a consequence:

‘[...] to acknowledge that an institution can establish secondary legal bases, whether for the purpose of strengthening or easing the detailed rules for the adoption of an act, is tantamount to according that institution a legislative power which exceeds that provided for by the Treaties’³⁵⁸.

Nevertheless, the CJEU found the act valid – in facts and law –, and invalidated it since Article 18(2) of the VIS LEA Decision should have been interpreted by virtue of Article 39 of the 2002 TEU, i.e. the European Parliament should have been consulted³⁵⁹. Thus, the VIS LEA Decision was replaced by a new one³⁶⁰ enabling Member States’ designated authorities and Europol to access the VIS for the purpose of the prevention, detection, and investigation of terrorist offences and other serious criminal offences from 1 September 2013.

4.3. The VIS revised Regulation

The European Commission VIS evaluation of 2016 assessed the contribution that the VIS was bringing to the combatting of “visa shopping” and visa fraud thanks to the support of biometric technology³⁶¹. Such a positive evaluation, supported by the eu-LISA’s technical reports and the activity of the VIS Supervision Coordination Group, paved the way for the revision of the VIS Regulation. Notably, although long-stay visas were originally excluded from the VIS Regulation as they did not belong to the Schengen *acquis*³⁶², in the early 2000s the European Commission proposed granting long-stay visa holders freedom of movement

³⁵⁸ See the C-540/13, *European Parliament v Council of the European Union*, para. 32. The CJEU remembered that this solution was set for the in C-133/06, *European Parliament v Council*, 6 May 2008, EU:C:2008:257, with regard to a secondary legal basis legitimizing the adoption of legislative measures and should be applicable also for the executive acts that aggravate or exemplify the law-making procedure.

³⁵⁹ The same rationale was applied in the so-called *Europol* judgment analysed in Chapter 3.

³⁶⁰ Council Implementing Decision (EU) 2015/1956 of 26 October 2015 fixing the date of effect of Decision 2008/633/JHA concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, *OJ L* 284, 30.10.2015, pp. 146-148.

³⁶¹ See the Council of the EU, *Commission Staff Working Document executive summary of the evaluation Accompanying the document Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the Visa Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation*, 13530/16 ADD 1, Brussels, 21 October 2016.

³⁶² This gap made the Member States to recognise long-stay visa holders the possibility to move within their territories for a three-month period on the basis of the mutual recognition of the residence permits issued by the own Member State issuing the long stay visa. However, the mobility of long-stay visa holders was obstacle by the long delays though which Member States were issuing the residence permits. Therefore, the EU adopted a new form of visa (D+C) to enable the circulation of long-stay visa during the first three months form the entrance into the territory – see the Council Regulation (EC) No 1091/2001 of 28 May 2001 on freedom of movement with a long-stay visa, *OJ L* 150, 6.6.2001, pp. 4-5. This type of visa was differently implemented by the Member State and, in the end, the movement of long-stay visa owners still was an issue.

within the Schengen area in light of the principle of equivalence ‘[...] between long-stay and short-stay visas issued by the Member States fully implementing the Schengen acquis in order to overcome the present problems encountered by third-country nationals legally staying in a Member State with a long-stay visa [...] that a person can travel around in the Schengen area for short stays for three months in any half year with the document on the basis of which he is legally present in a Member State’³⁶³. As a consequence, the Convention implementing the Schengen Agreement was amended so as to impose a systematic check of the SIS II before the issuing of a long-stay visa. The Council suggested that the European Commission establish a centralised database of long-stay visas, residence cards, and residence permits³⁶⁴ to fill in the “information gaps” existing with respect to these categories of migrants. With the entry into force of the Treaty of Lisbon in 2009, the EU acquired a new competence on visas and other short-stay residence permits that significantly expanded the scope of the common visa policy³⁶⁵. The new VIS Proposal enriched the VIS’ purposes beyond the common visa and residence policies:

‘The VIS is an integral part of the Commission’s approach to managing data for borders, migration and security. It seeks to ensure that border guards, law enforcement officers, immigration officials and judicial authorities have the information they need to better protect the EU’s external borders, manage migration and improve internal security for all citizens’³⁶⁶.

The VIS revised Regulation³⁶⁷ pursues the following objectives: the facilitation of the visa application procedure; the facilitation and strengthening of checks at the external border crossing points, and the enhancement of internal security³⁶⁸. Furthermore, several ancillary purposes were added, including: the facilitation of identity checks of third-country nationals in

³⁶³ See the Council of the EU, *Proposal for a Council Regulation amending the Convention Implementing the Schengen Agreement as regards long-stay visas and alerts in the Schengen Information System*, 7094/09, Brussels, 2 March 2009.

³⁶⁴ See the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA, COM(2018) 302 final, Brussels, 16.5.2018.

³⁶⁵ See Article 77(2)(a) of the TFEU.

³⁶⁶ See the Proposal for a Regulation of the European Parliament and of the Council, COM(2018) 302 final, Brussels, 16.5.2018.

³⁶⁷ See “Le Parlement européen confirme les nouvelles règles du Système d’information sur les visas”, *Bulletin Quotidien Europe*, No. 12757, 8.7.2021. The VIS Regulation has been amended by Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System, *OJ L* 248, 13.7.2021, pp. 11-87, and Regulation (EU) 2021/1133 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EU) No 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 and (EU) 2019/818 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the Visa Information System, PE/45/2021/INIT, *OJ L* 248, 13.7.2021, pp. 1-10.

³⁶⁸ Article 2(1) of the VIS revised Regulation.

the territory of a Member State by immigration and law enforcement authorities; the identification of missing persons, and irregular migrants for the purposes of return; law enforcement authorities' access to VIS data for the prevention, investigation, detection or prosecution of serious crime and terrorism, while ensuring high standards of data protection and privacy and, finally, the gathering of statistics to support evidence-based EU migration policy making.³⁶⁹

The new VIS Proposal was underpinned by a huge legal framework that embraced: Article 16(2) TFEU; Article 77(2)(a), (b), (d), and (e) TFEU; Article 78(2)(d), (e), and (g) TFEU; Article 79(2)(c) and (d) TFEU; Article 87(2)(a) TFEU, and Article 88(2)(a) TFEU. Thus, the EU competences covered: the protection of personal data and the free movement of such data; visas and other short-stay residence permits; measures on checks at external borders; the gradual establishment of an integrated border management system; the protection of personal data and its free flow among Member States; the Dublin mechanism; the examination of asylum applications; partnership and cooperation with third countries for the purpose of managing inflows of people applying for asylum, or for subsidiary or temporary protection; the exchange of information for police cooperation purposes, and the Europol mandate³⁷⁰. Finally, the VIS revised Regulation was amended by two instruments: Regulation (EU) 2021/1134 is underpinned by Article 77(2)(a), (b), (d) and (e) and Article 87(2)(a), while Regulation (EU) 2021/1133 is backed up by Article 78(2)(e), Article 82(1)(d), Article 87(2)(a), and Article 88(2). The latter Regulation integrates the VIS's amendments and it was separately adopted due to the fact that it concerns non-Schengen *acquis* matters which affect the Member States' participation as we will analyse in Chapter V³⁷¹. Unfortunately, the reference to Article 16 TFEU was finally discarded.

According to the legislative Proposal, the VIS should have stored a new type of information that could be complemented by the exchange of information through the VIS Mail

³⁶⁹ Article 2(1) of the VIS revised Regulation.

³⁷⁰ For which purpose the EU Council rejected the European Parliament's proposal of introducing previous identification biometric checks according to the Prüm Decision – see the Council of the EU, *Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System – Statement of the Council's reasons – Adopted by the Council on 27 May 2021*, 5950/1/21 REV 1 ADD 1, Brussels, 28 May 2021, p. 12.

³⁷¹ Some hints are available in Council of the EU, *Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council amending Regulations (EU) No 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 and (EU) 2019/818 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the Visa Information System – Draft Statement of the Council's reasons*, 5951/21 ADD 1, Brussels, 20 May 2021.

communication mechanism in substitution of the existing communication channel (VISION). A major change concerned the storage of a digital copy of travel documents to “better check” documents at the borders³⁷² and to facilitate the readmission of third country nationals. Thus, the VIS will contribute to returning migrants irregularly staying within the Schengen area, which confirms the Union’s willingness to push for conditionality³⁷³ rather than the regularisation of irregular migrants as suggested by the European Economic and Social Committee. In the latter’s opinion:

‘The third-country nationals should be encouraged and assisted by the authorities to regularize their stay and consider returning to their place of origin’³⁷⁴.

Consequently, personal data can be exceptionally transferred or made available to third countries or international organisations for the purposes of return, resettlement, or law enforcement, as we will further analyse in Chapter VI³⁷⁵. As far as biometric data is concerned, biometric facial images of visa applicants would be introduced as ‘the basic rule in the visa procedure’³⁷⁶ which includes biometric identification as a subsidiary non-unique search, including within the asylum context. According to the VIS revised Regulation, facial images can be taken in-person, scanned from a photograph or extracted from the Machine-Readable

³⁷² Article 9(b)(7) of the VIS revised Regulation. Possibly, in the future, visa stickers will be replaced by a digital copy so that the latter also might be included in the VIS – see “La Commission européenne lance une consultation publique sur la numérisation des procédures d’acquisition de visas”, *Bulletin Quotidien Europe*, No. 12676, 12.3.2021.

³⁷³ See “Le Conseil de l’UE se penche sur le lien entre politique des retours et de réadmission, et utilisation de la politique des visas”, *Bulletin Quotidien Europe*, No. 12673, 9.3.2021. The European Commission presented its ‘black-list’ of non-cooperative third countries, namely Bangladesh, Irak et Gambie, on the 16 July 2021 – see “La Commission européenne propose de durcir la délivrance de visas de court séjour pour les ressortissants de trois pays tiers”, *Bulletin Quotidien Europe*, No. 12763, 16.7.2021 – which measures both the collaboration in voluntary readmission programs and in the proceeding for the identification of third country nationals. Other neighbouring countries have raised the European Commission’s attention – see “Libéralisation des visas, les ressortissants moldaves, géorgiens et ukrainiens posent des difficultés à certains États membres”, *Bulletin Quotidien Europe*, No. 12801, 30.9.2021. Yet, it is up to the Council of the EU to adopt the relevant decision suspending some of the benefits granted by the Visa Code – see “La Commission européenne à nouveau questionnée sur son action après de nouvelles allégations de refoulements de migrants”, *Bulletin Quotidien Europe*, No. 12807, 8.10.2021. Conversely, Cabo Verde has recently passed into the list of “good countries” – see “Feu vert au nouvel accord sur les visas de court séjour avec le Cap-Vert”, *Bulletin Quotidien Europe*, No. 12781, 2.9.2021.

³⁷⁴ See the Opinion of the European Economic and Social Committee on ‘Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation (EU) 2018/... (Interoperability Regulation) and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA’ (COM(2018) 302 final), EESC 2018/03954, *OJ C* 440, 6.12.2018, pp. 154-157, para. 1.6.

³⁷⁵ Article 31 of the VIS revised Regulation.

³⁷⁶ Council of the EU, *Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System – Draft Statement of the Council’s reasons*, 5950/21 ADD 1, Brussels, 20 May 2021, p. 10.

Zone of the travel document³⁷⁷. However, in order to avoid any inaccuracy that may derive from morphing technology, the in-person taking of facial images should be preferred³⁷⁸.

As for dactyloscopy data, the minimum age for fingerprinting has been lowered to six years³⁷⁹. On this point, the European Commission maintained that children's fingerprinting would have been reliable on the basis of new advances in technology that guarantee the accuracy of biometric checks of children between six and twelve years old. Moreover, the European Commission stressed that the need to collect the minors' data would support the identification of victims of trafficking, missing children, and unaccompanied minors seeking asylum. It should be positively noted that the European Parliament complemented the proceeding presented by the European Commission with a child-friendly and child-sensitive approach that includes the mandatory presence of an adult, a guardian, or a person trained to safeguard the best interests of the minor.

In addition to the novelties analysed so far, the VIS revised Regulation provides for the insertion of automated checks against other databases following the wave of the new EES and the ETIAS Regulations. Automated checks are regulated under Article 9a of the revised VIS Regulation as soon as a VIS application is created:

‘When deciding whether to issue or extend a long-stay visa or residence permit, a number of automated checks will be launched using the interoperability components (the ESP) to detect whether an EU or Interpol database contains any evidence that the person could pose a threat to the security of one of the Member States. The Member State issuing the document will have to follow up on any hit in accordance with existing EU and national law’.

The hits are triggered against the other large-scale IT systems³⁸⁰, Europol data, and Interpol databases on SLTD and on TDAWN. They shall be verified by pre-established competent authorities: while visa authorities have access to the application files stored in VIS and to the ones held by the other databases³⁸¹, access by law enforcement authorities is filtered by the so-

³⁷⁷ Article 5(1)(b) of the VIS revised Regulation.

³⁷⁸ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA - Mandate for negotiations with the European Parliament*, 15726/18, Brussels, 19 December 2018, p. 20.

³⁷⁹ Article 22a(2) of the VIS revised Regulation. It shall be noted that the possibility to lower the age limit to zero years old was also contemplated in the Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA, SWD(2018) 195 final, Brussels, 16.5.2018.

³⁸⁰ As far as ECRIS-TCN is concerned, the hits relate to convictions for serious crimes and terrorism registered in the previous fifteen years and twenty-five years respectively.

³⁸¹ See Article 9a of the VIS revised Regulation.

called VIS designated authorities that must verify whether the identity of the applicant in the application file corresponds to the data stored in the other consulted databases³⁸². The hits resulting against the ETIAS' Watchlist and the SIS II "sensitive alerts" are verified by the ETIAS National Unit and the SIRENE Bureau respectively³⁸³. In parallel, the visa processing will be equipped with an algorithm that calculates "risk-indicators" based on previous statistics 'generated from other relevant border management and security databases'³⁸⁴ in order to assess security, illegal immigration, or high epidemic risks.

The icing on the cake of the VIS revised Regulation concerns its new architecture and, specifically, the integration of the VIS into the interoperability infrastructure: not only will the VIS exploit some of the interoperability tools to perform its functions – such as the ESP to carry out its automated checks³⁸⁵ – as advanced above, but it will also share the hardware and software of the EES and the ETIAS in light of the principle of cost-effectiveness³⁸⁶. In addition, the VIS Central System, the VIS National Interfaces, and the VIS communication infrastructure will be supported by a web service and carrier gateway suggesting that, on the one hand, the visa proceeding will be digitalised so that, in the future, it should be possible to submit individual visa requests through the web; and, on the other hand, carriers will have access to the VIS data with a 'ok/not ok' answer and through the carrier gateway, as is already the case for the ETIAS and the EES. In any case, it is still too early to jump to any study of the interoperability package as we now have to turn to the other three large-scale IT systems³⁸⁷.

³⁸² For which Member States can discretionally choose more than one authority, including the SIRENE Bureaux, by virtue of Article 9d of the VIS revised Regulation. Previously, Central Access Points according to Articles 9c and 9ca of the Council of the EU, 15726/18, Brussels, 19 December 2018.

³⁸³ See Articles 9e and 9f of the VIS revised Regulation, and on the SIS II sensitive alerts see Chapter V.

³⁸⁴ Council of the EU, 5950/21 ADD 1, Brussels, 20 May 2021, p. 11.

³⁸⁵ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA – Amendment to the mandate for negotiations with the European Parliament*, 8787/20, Brussels, 17 June 2020.

³⁸⁶ See Article (2a) in the European Parliament legislative resolution of 13 March 2019 on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No. 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA, COM(2018) 0302, Brussels, 13.03.2019.

³⁸⁷ To be noted that the documents concerning the forthcoming systems – specifically, the EES and the ETIAS – that have been retrieved from the EU Council register available on-line, do not show the position of the Member States' delegations which translates into a major loss of transparency on the negotiations surrounding the harsh world of large-scale IT systems.

5. Entry-Exit System (EES)

5.1. The 2008 Proposals on the EES and the Registered Traveller Programme

In 2008³⁸⁸ the European Commission presented the first smart borders package which encompassed the creation of an EES and a Registered Traveller Programme (RTP), while the possibility of introducing an Electronic Travel Authorisation System (ESTA) was taken under consideration. Soon afterward, the European Commission presented a first feasibility study on the creation of a system that would have enabled Member States to detect persons staying in the Schengen area beyond the authorised period in the case of short stays³⁸⁹. The first legislative measure came in 2013³⁹⁰, following the mandate endorsed by the European Commission under the Stockholm Programme³⁹¹. The Proposal was underpinned by Articles 74, and 77(2)(b) and (d) of the TFEU. The former:

‘[...] provides the appropriate legal basis for setting-up and maintaining the EES and for procedures for the exchange of information between Member States, ensuring cooperation between the relevant authorities of the Member States’ as well as between those authorities and the Commission in the areas covered by Title V of the Treaty’³⁹².

The latter set forth the EU competence on checks at the external borders, as well as the development of standards and procedures in carrying out those checks under the aegis of the gradual establishment of an integrated management system for external borders.

³⁸⁸ See the Council of the EU: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Preparing the next steps in border management in the European Union, COM(2008) 0069 final, Brussels, 13.02.2008, paras. 2, 3 and 4, criticised by the Preliminary Comments of the EDPS on - *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, “Preparing the next steps in border management in the European Union”*, COM(2008) 69 final; - *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, “Examining the creation of a European Border Surveillance System (EUROSUR)”*, COM(2008) 68 final; - *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, “Report on the evaluation and future development of the FRONTEX Agency”*, COM(2008) 67 final, Brussels, 3.03.2008.

³⁸⁹ See the Council of the EU, *Presidency project for a system of electronic recording of entry and exit dates of third-country nationals in the Schengen area*, 12251/08, Brussels, 28 June 2008. As a last resort, the system would have supported the collection of data on migration flows and overstayers and it would have improved the management of economic migration.

³⁹⁰ See the Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union, COM(2013) 95 final, Brussels, 28.02.2013, and the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562(2006) as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP), COM(2013) 96 final, Brussels, 28.02.2013.

³⁹¹ The Stockholm Programme — An open and secure Europe serving and protecting citizens, OJC 115, 4.5.2010, pp. 1-38.

³⁹² See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union*, 6928/13, Brussels, 28 February 2003, p. 6.

The European Commission Proposal of an EES underlined that at the external borders both EU citizens and third country nationals would be subject to a minimally intrusive check '[...] consisting in the verification of the travel document in order to establish the identity of the person'³⁹³. However, the latter were also requested to declare the purpose of their stay, evidence sufficient means of subsistence, and were to be checked against the SIS II and national databases³⁹⁴. It must be recalled that, traditionally, the entry of third country nationals into the Schengen area was sealed with a stamp on their travel document, yet no mark was recorded for their exit. As a consequence, people that overstayed after a short stay visit of ninety days without exceeding a period of one hundred and eighty days could not be detected. The Commission's Proposal aimed at modernising border checks by ensuring that the automated border crossing points were able to read the Machine-Readable Zone of the traveller's documents, or their biometric data³⁹⁵. These checks would have captured the records on the migrant's entries and exits from the Schengen area in order to calculate each travellers' authorised stay³⁹⁶. After the period expired, an automated system should have sent an alert to the competent authorities designated by the Member States³⁹⁷.

The Proposal was accompanied by the establishment of the RTP³⁹⁸ and an amendment to the Schengen Borders Code³⁹⁹. The RTP would have created a Central Repository where, on a voluntary basis, travellers could register at consulates, common application centres and at the border crossing points. Travelers would be assigned a token – a machine readable card – with a unique identifying number to be swiped on arrival and departure through an automated gate at the border (an eGate). The eGate should have read the travellers' tokens, travel documents (and visa stickers if applicable) and fingerprints. To allow the crossing of the external borders,

³⁹³ *Ibid.*, p. 1.

³⁹⁴ Article 6 of the Schengen Borders Code.

³⁹⁵ This would have substituted the traditional stamps printed in the travel documents of third country nationals, though Member States were initially concerned by this novelty – see the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union*, 11143/13, Brussels, 20 June 2013, p. 4.

³⁹⁶ It shall be noticed that Spain and Latvia pushed for the enlargement of the scope of EES to all third country nationals, including the holders of residence permits to check the periods of staying granted by the other Member States – see the Council of the EU, 6928/13, Brussels, 28 February 2003, and Council of the EU, 9863/13, Brussels, 28 May 2013, p. 4.

³⁹⁷ See Articles 9, 10 and 7 respectively of Council of the EU, 6928/13, Brussels, 28 February 2003. The delegations also contemplated the possibility that the records of entry and exit may have been converted into an alert in the SIS II, see the questionnaire referred to in the following footnote No. 161.

³⁹⁸ Proposal for a regulation of the European Parliament and of the Council establishing a registered traveller programme, COM(2013) 97 final – 2013/0059 (COD).

³⁹⁹ See the consequential amendments proposed in the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP)*, 6931/13, Brussels, 28 February 2013.

the data should have been compared with the Central Repository, the VIS⁴⁰⁰, and other databases⁴⁰¹.

The EES was accessible to border authorities to perform individual checks at the external borders⁴⁰² also through a biometric search in the system⁴⁰³. But the EES was also accessible to many other authorities such as: visa authorities before they issued a visa⁴⁰⁴; competent authorities examining RTP applicants⁴⁰⁵, and national authorities competent for verifying the conditions of entry and stay in the Member States' territories – both through biometric verification and identification⁴⁰⁶. The possibility to give access to law enforcement authorities for the combating of terrorism and other serious crimes was abandoned by the European Commission for a couple of years, as they waited for the results of the implementation of the VIS⁴⁰⁷. Such a possibility was presented as one of the four possible options for the implementation of the EES, yet, it should have been accompanied by an extension of the retention period to five years for all categories of travellers⁴⁰⁸. The European Commission specified that:

⁴⁰⁰ During the negotiations, some delegations expressed the willingness to interconnect the VIS and the EES so that the visa information stored in the former would be made available in the latter. It is interestingly to note that the European Commission clearly stated that the VIS and the EES could not be linked since their searches are different and they also have different legal basis, yet it asked the delegations more time to reflect on the possibility to interconnect these databases in case of revocation of a short-stay permit – see the Council of the EU, 11143/13, Brussels, 20 June 2013, pp. 6 and 9.

⁴⁰¹ The RTP was criticised by the EDPS since the proposal entailed discrimination between frequent travelers that would have been registered in the RTP and, therefore, they would be considered as “low risky travelers” while the other one, merely for the fact of travelling less, would be turned out to be “high risky travelers” – see the Council of the EU, *Opinion of the European Data Protection Supervisor on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme*, 10679/13, Brussels, 24 July 2013, p. 20.

⁴⁰² See Article 15 of the Council of the EU, 6928/13, Brussels, 28 February 2003.

⁴⁰³ *Ibid.*, Article 1.

⁴⁰⁴ *Ibid.*, Article 16.

⁴⁰⁵ As proposed by the European Commission in the Proposal for a Regulation of the European Parliament and of the Council, COM(2013) 97 final, Brussels, 28.2.2013.

⁴⁰⁶ See Article 18 and 19 of the Council of the EU, 6928/13, Brussels, 28 February 2003.

⁴⁰⁷ See the Council of the EU, *Commission Staff Working Document, Executive Summary of the Impact Assessment, Proposal for a Regulation of the European Parliament and of the Council establishing an entry/exit system to register entry and exit data of third-country nationals crossing the external borders of the Member States of the European Union*, 6928/13 ADD 2, Brussels, 28 February 2013, p. 7.

⁴⁰⁸ On the contrary, two different periods of storage of personal data were established: Six months as a general norm, and five years only for travelers that did not exit the territory in due time – see the Council of the EU, *Commission Staff Working Document Impact Assessment Proposal for a Regulation of the European Parliament and of the Council establishing an entry/exit system to register entry and exit data of third-country nationals crossing the external borders of the Member States of the European Union*, 6928/13 ADD 1, Brussels, 28 February 2013. As for VIS, a transitional period was allowing Member States to carry out the verification at the borders crossing point through the visa sticker. Article 50(5) of the VIS Regulation enabled the European Commission to issue a first report on the use of fingerprints at the external to assess whether the verification process had entailed excessive waiting times.

‘[...] the necessity and proportionality of the use of this data must be clearly demonstrated with solid evidence and the access must be combined with appropriate safeguards and limitations’⁴⁰⁹.

Nevertheless, Member States strongly supported the enlargement of the EES’s scope to include law enforcement authorities as an “ancillary” purpose for the management of external borders⁴¹⁰ and an agreement was finally reached⁴¹¹. This would have entailed a reference to Article 87(2)(a) TFEU and, for Europol, of Article 88(2)(a) TFEU, which raised concerns on whether the Regulation could have been considered as a development of the Schengen *acquis*, or not⁴¹². The Member States’ delegations pushed for a widespread debate on the access of law enforcement authorities to the new system, which spurred the Council Presidency to retrieve more information from the Member States with regard to the access they were already granting their police forces to their respective national databases⁴¹³. Unfortunately, the Member States’ replies are not accessible to the public⁴¹⁴; in any case, access by law enforcement authorities should have been proportionated and limited to what was strictly necessary for the purposes of attaining the objectives pursued⁴¹⁵. Hence, the Presidency suggested the adoption of the VIS

⁴⁰⁹ See the Council of the EU, 6928/13 ADD 2, 28 February 2013, p. 7.

⁴¹⁰ See the positions of the delegations in the Council of the EU, 9863/13, 2 Brussels, 8 May 2013, pp. 2 and 5. Yet, the European Commission confirmed that the proportionality test might have failed because of the huge amount of personal data collected in the EES as well as the benefits that would have come from the use of EES for combatting crime. Member States were again consulted through a questionnaire that is partially accessible, but it shows how some of the Member States were already managing law enforcement access at the national level – see the Council of the EU, *Draft Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union - Access for law enforcement purposes*, 8743/15, Brussels, 19 May 2015.

⁴¹¹ On the 24 September 2013 according to the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union*, 17536/13, Brussels, 13 December 2013.

⁴¹² See the Council of the EU, *Draft Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union - Access for law enforcement purposes: Summary and comments by the Presidency regarding answers provided by the Member States to the questionnaire of the former Greek Presidency and discussion on the ways forward*, 13225/14, Brussels, 17 September 2014, p. 2.

⁴¹³ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union – Questionnaire*, 12107/13, 15 July 2013, and Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union – Questionnaire*, 12107/13, 15 July 2013, 14066/13, Brussels, 1 October 2013.

⁴¹⁴ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union – Access for law enforcement purposes: Summary of the replies to the questionnaire*, 13680/13, Brussels, 10 October 2013.

⁴¹⁵ The Presidency expressly referred to the C-293/12 and C-594/12, *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General*. See the Council of the EU, *Draft Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit*

and the Eurodac approach whereby “verifying authorities” should have surveilled the law enforcement authorities’ access to the EES⁴¹⁶. The “cascade” approach envisaged by the Eurodac was initially discarded since entry and exit records were not available in other databases such as the VIS, the SIS II and the Prüm framework⁴¹⁷.

Granting the access to the EES to law enforcement authorities presented a setback in two areas: first, Member States had been pushing for the insertion of a huge number of biometrics since the very beginning of its implementation⁴¹⁸ and, second, they sought the extension of the retention period⁴¹⁹. Indeed, one of the main added values of the EES consists of the storage of biometric data of visa-exempt third country nationals⁴²⁰. The collection of fingerprints would have facilitated the identification of visa-exempt third country nationals found in the territory of the Member States without an identity document. In this sense, the EES Proposal introduced

data of third country nationals crossing the external borders of the Member States of the European Union, 10720/14, Brussels, 12 June 2014, p. 4.

⁴¹⁶ *Ibid.*: ‘For law enforcement purposes, it seems that the most important data to have access to are the fingerprints because they would enable identifying a suspect’, p. 9 and the document on the Council of the EU, *Access for law enforcement purposes to the Entry/Exit System*, 11337/1/14 REV 1, Brussels, 16 July 2014.

⁴¹⁷ See the Council of the EU, 13225/14, Brussels, 17 September 2014, pp. 3 and 4.

⁴¹⁸ Ten fingerprints instead of four as it was proposed for the RTP. Furthermore, delegations also proposed to process facial images, yet some concerns arose since the capture of facial images at the borders might have augmented the waiting periods of travelers. See the positions of was proposed by Germany, Greece, and The Netherlands in the Council of the EU, 9863/13, Brussels, 28 May 2013, p. 7. The European Commission proposed a transitional period of three years from the entry into operation of the systems in which only alphanumeric data should have been recorded in the EES. This would have allowed the Member States to adapt their process at the national borders – see Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union*, 15969/13, Brussels, 18 November 2013.

⁴¹⁹ It was proposed a five years period of storage though, in the end, a three years period was agreed unless no exit record is recorded – see Article 34 of the Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, *OJ L* 327, 9.12.2017, pp. 20-82 (EES Regulation hereinafter).

⁴²⁰ See the Member States’ comments in the Council of the EU, *Presidency project for a system of electronic recording of entry and exit dates of third-country nationals in the Schengen area*: 13403/08, Brussels, 24 September; 13403/08 ADD 1, Brussels, 25 September; 13403/08 ADD 2, Brussels, 25 September of 2008; 13403/08 ADD 3, Brussels, 15 October 2008; 14334/08, Brussels, 16 October 2008; 13403/08 ADD 4, Brussels, 20 October 2008, and 13403/08 ADD 5, Brussels, 21 October 2008. Among the Member States, Slovenia expressed a strong position against the systematic storage of biometric data of visa exempt third country nationals, by assuming that:

‘[...] capturing fingerprints from all third country nationals entering the territory of Member States is not proportionate to the aims we are heading. The sole purpose of capturing the fingerprints is to be able to identify third country nationals within the territory of the Member States who have no documents (no possibility to identify them using other means). For the purpose of identifying third country nationals who have exceeded their stay and have their documents (at the border crossing points or within the territory) capturing of fingerprints at entry and exit is not necessary as this aim can be pursued by capturing only alphanumeric data when third country national enters Member State’.

Unfortunately, not all the questionnaires and replies submitted to the delegations are available – see the document partially accessible to the public Council of the EU, *Questionnaire on the possible creation of a system of electronic recording of entries and exits of third country nationals in the Schengen area*, 8552/09, Brussels, 21 April 2009.

the concept of “identification” in terms of biometric recognition – i.e., a one-to-many match – as ‘[...] the process that enables the identification of the individual through a database search against multiple sets of data’⁴²¹. In the end, the EES resulted in a patchwork of EU policies on the management of those overstaying their visas that the EDPS strongly criticised. In his words:

‘[...] it appears that the database is created without the existence of a comprehensive policy, and even in order to find out whether and how such an EU policy should be developed’⁴²².

By identifying those overstaying their visas, the EDPS highlighted that many different policies, including general visa policies and those dealing with irregular migration, would have been involved alongside those that directly concerned borders. Furthermore, it was not clear how the gathering of statistics on the entries and exits of third country nationals would have contributed to EU policies⁴²³. In the EDPS’ opinion, the Proposal should have further elaborated on the impact that a centralised EES would have had on visa policies, irregular migration and border checks. The authority invited an in-depth analysis of existing IT systems before a new system was developed as their purposes might have ended up overlapping with one another. The EDPS further commented that the multiplication of databases in the field of border management would have hindered the exercise of the data protection rights of all individuals and further attention should have been paid to this issue. In this sense, the information provided to migrants in order to assist them in identifying the Member State responsible for entering their data was crucial so as to exercise their right to access, modify, and erase their data and, as a last resort, their access to a remedy.

⁴²¹ See Article 5(10) of the Council of the EU, 6928/13, Brussels, 28 February 2003. At that time, visa-exempt third country nationals from twelve years old ahead were asked to provide ten fingerprints for the creation of a new identity file in the system.

‘While acknowledging the advantages of collecting biometrical data, the EESC notes the impact that fingerprints has on regular or non-regular travellers. The psychological impact is detrimental to the motivation to travel and generally to the individual’s relationship with the host society. Moreover, fingerprints are traditionally associated with criminal activities and with policing practices. The EESC calls for further consideration of biometrical data gathering as part of the two programmes and of ways to limit its adverse effects’.

in the Opinion of the European Economic and Social Committee on the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP), Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme*, 10704/13, Brussels, 10 June 2013, p. 6.

⁴²² See the Council of the EU, 10679/13, Brussels, 24 July 2013, p. 8.

⁴²³ See Article 4 and 40 of the Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union, COM(2013) 095 final, Brussels, 28.02.2013.

The negotiations around the EES package were interrupted as ‘[...] the co-legislators voiced technical, cost-related and operational concerns on the design of the systems’⁴²⁴. The European Commission reported that the unresolved issues were due to: the limited number of users and the administrative burden of implementing the RTP; the length of the data retention period in the EES; the choice of the biometric identifiers; the extent to which the national EES could be integrated and/or reused; the need for enhanced synergies and/or interoperability with existing systems used during border controls, and the possibility of law enforcement authorities accessing the system. As a consequence, the European Commission launched a “proof of concept” exercise that took place between 2014 and 2015 and comprised a Technical Study on Smart Borders and a testing phase (the ‘Pilot’)⁴²⁵.

5.2. The 2017 Regulation on the establishment of the EES

After the 2015 humanitarian crisis, a revised smart border package⁴²⁶ was presented following the wake of President Juncker’s speech part of which said:

‘[...] the Commission proposes to strengthen the Schengen Borders Code so that every person entering the Schengen area – whether they are an EU national or a third country national – will undergo a security check against national and European databases. And checks on all individuals will now be mandatory when exiting the European Union as well. These are the costs of a riskier world, and they cannot be avoided’⁴²⁷.

The new package was expected to create a more conformable environment with new political, legal, and institutional perspectives⁴²⁸: the VIS had been in operation since 2015, and new technological solutions would enable the rapid reading of biometrics. Also, the possibility to take advantage of the new Internal Security Fund and, as part of this, the border component of the Fund – that allocated 791 million euros for the development of the Smart Borders package – facilitated the discussions with the delegations. This second Smart Borders package sought to amend the Schengen Borders Code so as to insert systematic checks at the external borders and revisited the idea of the necessity of the implementation of the EES. As a consequence, the European Commission decided to revise its former Proposals⁴²⁹.

⁴²⁴ See the Commission Staff Working Document Impact Assessment, Impact Assessment Report on the establishment of an EU Entry Exit System, SWD(2016) 115 final, Brussels, 6.4.2016, p. 1.

⁴²⁵ See the eu-LISA’s report on *Smart Borders Pilot Project. Report on the technical conclusions of the Pilot*, Tallin, 2015.

⁴²⁶ See the Communication from the Commission to the European parliament and the Council, Stronger and Smarter Information Systems for Borders and Security, COM(2016) 0205 final, Brussels, 6.4.2016.

⁴²⁷ Speech by President Juncker at the European Parliament Plenary – Preparation of the European Council meeting of 17-18 December 2015, Strasbourg, 16 December 2015.

⁴²⁸ See the Commission Staff Working Document Impact Assessment, SWD(2016) 115 final, Brussels, 6.4.2016.

⁴²⁹ See the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System, COM(2016) 0196 final, Brussels, 6.4.2016, and the Proposal

The first Proposal on the establishment of the EES sought to record the entry and exit of all third country nationals authorised to stay within the territories of the Member States on a short stay⁴³⁰. In this sense, the EES would integrate the biggest source of information on third country nationals, including visa and visa-exempt travellers, by which it materially impacts the migrants' rights to privacy and to the protection of their personal data⁴³¹.

The EES Proposal pursued two main objectives: first, assisting in the fight against irregular migration; and second, the prevention and combatting of terrorism and serious crimes⁴³². Hence, the proposed Regulation was underpinned by Articles 74, 77(2), 82 (1)(d), and 87(2)(a) TFEU. Although the 2013 work paved the way for the revised initiative, it shall be noted that the purposes of the new legislative measure consisted of the improvement of the quality of external borders checks⁴³³ in order to fight against irregular migration as well as terrorism and serious crimes. In response to the EDPS's previous comments, the European Commission stated that:

‘[n]o new policy in new areas will be developed. The proposal is part of the continuous development of the Integrated Border Management Strategy of the European Union’⁴³⁴.

Nevertheless, the EDPS recalled that even if different “ancillary” purposes could have been added, border management should have remained the primary purpose of the EES. Still, the twofold nature of the EES may be maintained by looking at the regimes established for the transferral of personal data to third countries and international organisations which included both the provision of information to border authorities or immigration authorities under the GDPR and the LED⁴³⁵.

for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011, COM(2016) 0194 final, Brussels, 6.4.2016.

⁴³⁰ Indeed, by extending the scope of application not only to Member States fully applying the Schengen *acquis*, but also to Bulgaria, Romania, Croatia and Cyprus, the period of permanence in these four Member States should have been taken into account too, though they still do not participate in the Schengen cooperation.

⁴³¹ See the Opinion of the EDPS No. 06/2016 on the *Second EU Smart Borders Package Recommendations on the revised Proposal to establish an Entry/Exit System*, Brussels, 21.09.2016, that explicitly makes reference at p. 9, to the historical joined cases C-293/12 and C-594/1239, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*.

⁴³² See the list of purposes under Article 5 of the Proposal for a Regulation of the European Parliament and of the Council, COM(2016) 0194 final, Brussels, 6.4.2016, today Article 6 of the EES Regulation.

⁴³³ See Article 23 of the EES Regulation.

⁴³⁴ See the Commission Staff Working Document Impact Assessment, SWD(2016) 115 final, Brussels, 6.4.2016, p. 19.

⁴³⁵ See Article 39 of the EES Regulation that allows the designated authorities to transfer the information according to the LED, despite the fact that the European Parliament proposed its deletion – see the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of, entry data of third country nationals crossing the external borders of Member States of the European Union and determining the conditions for access to the EES for law enforcement*

All these policies aimed at identifying third country nationals⁴³⁶. In the European Commission's Proposal, issues related to the identification of third country nationals were firstly linked to the access to the system by law enforcement authorities and Europol for the combating of terrorism and serious criminal offences⁴³⁷. Indeed, the EES Regulation expressly provides for the possibility to also launch identity searches with latent fingerprints, i.e. those that are generally used during police investigations⁴³⁸. In the elaboration of the EES Proposal, the detection of undocumented criminals or persons using multiple identities was highlighted as a particular problem, since this could easily circumvent the SIS II alert mechanism⁴³⁹. Besides, while third country nationals subject to a visa for entry could be identified through the VIS⁴⁴⁰, visa-exempt third country nationals remained undetected. Nevertheless, the inclusion of visa holders' data in the EES was justified along different lines: the VIS lacked a calculator that would have determined the duration of the stay in the Member States' territories⁴⁴¹. The

purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011 - Article 38 and 38a, 10114/17, Brussels, 8 June 2017, and Council of the EU, Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of, entry data of third country nationals crossing the external borders of Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011 - Article 38 and 38a, 10361/17, Brussels, 15 June 2017.

⁴³⁶ See Article 6(1)(b) and (c) of the EES Regulation.

⁴³⁷ See Chapter IV of the Proposal for a Regulation of the European Parliament and of the Council, COM(2016) 0194 final, Brussels, 6.4.2016, still Chapter IV of the EES Regulation.

⁴³⁸ See Article 32(4)(a) of the EES Regulation.

⁴³⁹ See the Commission Staff Working Document Impact Assessment, SWD(2016) 115 final, Brussels, 6.4.2016, para 1.4.

⁴⁴⁰ The European Commission reported that VIS was accessed by law enforcement authorities to identify people died in a violent way or for human being trafficking, terrorism or drug trafficking purposes, see the Council of the EU, 10114/17, Brussels, 8 June 2017, and Council of the EU, 10361/17, Brussels, 15 June 2017.

⁴⁴¹ The implementation of the EES raised another point of discussions on the existing visa waiver bilateral agreements celebrated between Member States and third countries by virtue of Article 20 of the Convention implementing the Schengen Agreement. These agreements may confer to third country nationals the right to stay beyond ninety days in a period of one hundred eighty days. While the European Commission strongly condemned the celebration of those treaties in the light of the establishment of a common policy of visa under Articles 77(2)(a) and (c) of the TFEU, Member States opposed the primacy of their diplomatic relationship. On the matter – see the Council of the EU, *Note from the French authorities on Article 54 (bilateral agreements) of the draft Regulation establishing an Entry/Exit System*, 14562/16, 18 November 2016. *Law enforcement access to EES and bilateral agreements were already the last two points of discussions until the end, see the Entry Exit (EES): a) Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of, entry data of third country nationals crossing the external borders of Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011 b) Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 2016/399 as regards the use of the Entry/Exit System - Progress report*, 15350/16, Brussels, 7 December 2016. Hence, Article 11(6) of the EES Regulation establishes that the EES calculator shall take into account the extension of the authorized stay even if it exceeds the period of ninety days in any 180-day period. Also confront the List of Member States' bilateral visa waiver agreements with third countries allowing for an extension of the period of stay in accordance with Article 20(2), point (b), of the Convention implementing the Schengen Agreement, *OJ C 130*, 8.4.2019, pp. 17-52.

need to identify criminals through a one-to-many search⁴⁴² by law enforcement authorities and Europol⁴⁴³ legitimised their access to the EES. Despite Europol's access to the system, the reference to 82(1)(d) TFEU was discarded in the final text, most likely due to the CJEU jurisprudence affirming that the access of these authorities should be proportionate, narrowly targeted, and based on suspicions surrounding a specific person⁴⁴⁴. In order to supervise the lawful access to the EES of “designated authorities” and Europol⁴⁴⁵, the Eurodac, and the VIS examples were followed and independent verifying authorities within the Central Access Point were pre-established in each Member State⁴⁴⁶. The access of designated authorities to the EES drew the attention of the EDPS that recommended, once again, that police cooperation should have been viewed as an ancillary purpose of the system⁴⁴⁷.

As for police objectives, one of the last points of discussion concerned the so-called “two-steps” or cascade approach that would have obliged the designated authorities and Europol to consult existing national databases and other decentralised ones – such as the one set forth in the Prüm Decision – prior to accessing the EES, and, in case of a hit, access to the EES would be prohibited. Member States fought unsuccessfully to have direct access to the EES⁴⁴⁸ and, today, the two-step approach can be skipped only when there are reasonable grounds to believe

⁴⁴² See Article 32 of the EES Regulation, and recital (30) that refers to ‘unknown suspects, perpetrators or victims of terrorist offences or other serious criminal offences’ for which a biometric identification search could have been launched in the system.

⁴⁴³ See Article 33 of the EES Regulation.

⁴⁴⁴ C-203/15 and C-698/15, *Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis*.

⁴⁴⁵ See the definition of Article 3(26) of the EES Regulation. Unfortunately, and although the Proposal did provide so, the provision that imposed the publication of the list of these authorities in the *OJ* was discarded – see the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*, 9578/16, Brussels, 31 May 2016, pp. 31 and 32.

⁴⁴⁶ One for law enforcement and one for Europol, see Articles 32 and 33 of the EES Regulation. The EDPS recommended that the Central Access Point should have been placed outside the organisation of law enforcement authorities and Europol – see the Opinion of the EDPS No. 06/2016 on *the Second EU Smart Borders Package Recommendations on the revised Proposal to establish an Entry/Exit System*, Brussels, 21.09.2016, p. 21. They are regulated under the Commission Implementing Decision (EU) 2018/1547 of 15 October 2018 laying down the specifications for the connection of the central access points to the Entry/Exit System (EES) and for a technical solution to facilitate the collection of data by Member States for the purpose of generating statistics on the access to the EES data for law enforcement purposes, C/2018/662, *OJ L* 259, 16.10.2018, pp. 35-38.

⁴⁴⁷ See Opinion of the EDPS No. 06/2016 on *the Second EU Smart Borders Package Recommendations on the revised Proposal to establish an Entry/Exit System*, Brussels, 21.09.2016, p. 19.

⁴⁴⁸ See Article 29 of the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011 Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 2016/399 as regards the use of the Entry/Exit System - Preparation of further steps*, 14700/16, Brussels, 24 November 2016, p. 10.

that the search would not lead to the verification of the individual's identity or in cases of urgency⁴⁴⁹. Some delegations remained unsatisfied with the outcomes of the discussions⁴⁵⁰ and relied on interoperability to 'hopefully [find] a solution'⁴⁵¹.

On the contrary, and despite the fact that the European Commission repeatedly underlined that the EES Proposal did not aim at resolving the humanitarian crisis that hit the EU in 2015, the question of "undocumented" migrants was considered even in the very early preparatory works⁴⁵². Even if Member States had kept their national systems for recording entries and exits⁴⁵³, the EU central database could have brought the added value of detecting third country nationals entering through one Member State and exiting from another⁴⁵⁴. Specifically, the EES Regulation safeguards the provision of an "alert bell" that can warn the competent authority when the maximum duration of a stay has expired⁴⁵⁵, it is also presumed that the third country national irregularly remains in the EU when no exit record is registered in the system after the expiration period⁴⁵⁶. In this sense, the EES is supposed to support the identification of all *sans papier* overstayers, including where these individuals are refused asylum⁴⁵⁷. Indeed, the

⁴⁴⁹ See Article 32(2), last paragraph, of the EES Regulation.

⁴⁵⁰ The delegations asked the Presidency to "freeze" the negotiations until the report of the HLEG on interoperability would have been issued, but the Council of the EU rejected this possibility by stating that: 'Taking into account the fact [...] Art. 29 of the draft EES Regulation has already been modified to soften the access conditions for law enforcement authorities to the maximum extent compatible to the current legal and judicial framework, the Presidency trusts that delegations will be able to support the Presidency compromise text on this issue' – see the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of, entry data of third country nationals crossing the external borders of Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011. Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 2016/399 as regards the use of the Entry/Exit System - Partial mandate to open interinstitutional negotiations with the European Parliament*, 15063/16, Brussels, 6 December 2016, pp. 4 and 5.

⁴⁵¹ See the Austrian position in Council of the EU, *Draft Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System (first reading) - Adoption of the legislative act = statements*, 14091/17 ADD 1, Brussels, 10 November 2017.

⁴⁵² See the Commission Staff Working Document Impact Assessment, SWD(2016) 115 final, Brussels, 6.4.2016, p. 21.

⁴⁵³ See Article 38 of the EES Regulation for which Member States can retrieve an individual case and keep it in a national file '[...] in accordance with the purpose for which they were retrieved and with relevant Union law, in particular on data protection, and for no longer than strictly necessary in that individual case'.

⁴⁵⁴ Family members of EU citizens as well as national of a third country enjoying the right of free movement under Union law fall out of the scope of the EES Regulation pursuant to Article 2(3)(a) to (c). However, it shall be noted that during the negotiations the delegations supported the idea of enlarging the scope of EES to EU citizens too – see the position of the Czech Republic in Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*, 8446/16, Brussels, 2 May 2016.

⁴⁵⁵ See Article 12 of the EES Regulation.

⁴⁵⁶ See Article 20 of the EES Regulation that also allows the individual to prove that the data stored in the EES are inaccurate so as to rebut this presumption.

⁴⁵⁷ To this purpose, immigration authorities are the only ones with access to the list of overstayers that the EES shall elaborate in an automated manner following the provisions of the Commission Implementing Decision (EU)

possibility to grant asylum authorities access to the EES was also advanced in the EES negotiations in order to support their tasks in analysing an asylum request and, in case of refusal, to speed up the return procedure⁴⁵⁸. Although the Presidency discarded these provisions, delegations – fully supported by the Council and the European Commission⁴⁵⁹ – were still unsatisfied with the political agreement reached in the discussions⁴⁶⁰. Therefore, the EES would also be operational within the territories of the Member States to aid the return of irregular migrants⁴⁶¹. This approach had an important impact on the regulation of the biometric identification of third country nationals as it shifted from the external borders to the territories of the Member States⁴⁶². Biometrics identifiers are an important tool, not only in strengthening the relationship between the individual and the travel document at the border crossing points, but also for detecting identity fraud⁴⁶³, travel document fraud⁴⁶⁴ and to identify undocumented people moving within the Member States' territories⁴⁶⁵.

2018/1548 of 15 October 2018 laying down measures for the establishment of the list of persons identified as overstayers in the Entry-Exit System (EES) and the procedure to make that list available to Member States, C(2018)6665, OJ L 259, 16.10.2018, pp. 39-42.

⁴⁵⁸ See Articles 25a and 25b in the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*, 10880/16, Brussels, 6 July 2016, and Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*, 10113/1/17 REV 1, Brussels, 15 June 2017.

⁴⁵⁹ See the Council of the EU, *Draft Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (first reading) - Adoption of the legislative act = statements*, 14092/17 ADD 1, Brussels, 10 November 2017.

⁴⁶⁰ See the Austrian position for which '[t]he access of asylum authorities to the EES for reasons of identification of third country nationals as well as for reasons of process facilitation and returns would have constituted the central additional benefit if the EES' in Council of the EU, 14091/17 ADD 1, Brussels, 10 November 2017.

⁴⁶¹ At this stage, the exchange of information from the Member States to third countries of origin and transit becomes a crucial step to execute the return of third country nationals. See the Article 38 of the Proposal and on the identification of migrants for the purposes of return and in the outstanding literature the reflection of Sergio Carrera, *Implementation of EU Readmission Agreements Identity Determination Dilemmas and the Blurring of Rights*, New York, Springer International Publishing, 2016.

⁴⁶² See Article 27 of the EES Regulation that allows the access of immigration authorities to the EES.

⁴⁶³ The European Commission explained in its Commission Staff Working Document Impact Assessment, SWD(2016) 115 final, Brussels, 6.4.2016, that in case of a biometric match the individual would have been found to be registered in the database so the authority may have inferred that the system would be able to detect: if the individual is using the same identity in more than one travel document issued by one or several countries, or bi-nationals; if the individual already registered in the database has legally changed identity – change of name after marriage –, or if the individual is using several identities.

⁴⁶⁴ On the contrary, the European Commission discarded the possibility that visa sticker can be forged since the fingerprints taken at the border are matched with fingerprints provided at the moment of the visa application – the so-called verification procedure.

⁴⁶⁵ See Chapter V.

During the negotiations, the storage timeline of the files on individuals held on the EES, as well as the entries/exits records, were important points that were contested by the European Parliament. It was proposed by the European Commission that individual files containing identity data were to be stored for a period of five years and one day. Equally, the extension of the retention period of entry and exit records was set at five years following the day of the last entry/exit record so as to avoid re-enrolment as well as to support the creation of risk analysis reports⁴⁶⁶. In practice, the EDPS highlighted that, under this logic, people crossing Member States' borders more than once in a five-year period would have their data recorded on a permanent basis⁴⁶⁷. Along the same lines, overstayers would also have their data recorded for a period of five years starting from the day after the last day of their authorised stay. Since the same category of persons would have been issued an entry ban in the SIS II, the EDPS criticised the necessity of such a long retention period⁴⁶⁸. The retention period was then reduced thanks to the interinstitutional mediation activity of the European Parliament. Although the Parliament opted for a four-year period of retention for overstayers, and two years for third country nationals that would have respected the period of authorised stay, the span was lowered as follows: five years in case of overstayers, and three years for authorised staying and refusal of entries⁴⁶⁹.

The EES is expected to become the biggest centralised large-scale IT system that stores biometric data. Overall, the data items were reduced from thirty-six to twenty-six, which was especially welcomed by the EDPS; yet, the categories of biometric data stored therein⁴⁷⁰ have augmented and the optimal combination of data was found in the matching of facial images and four fingerprints – instead of ten fingerprints as proposed in 2013: while four fingerprints would be used in the enrolment phase to check if the third country national was already registered in the system, a facial image would be used for verification purposes upon subsequent entries. In any case, both fingerprints and facial images can be used for identification purposes⁴⁷¹. The EDPS noted that:

⁴⁶⁶ See Article 57 of the Proposal for a Regulation of the European Parliament and of the Council, COM(2016) 0194 final Brussels, 6.4.2016, pp. 20-82.

⁴⁶⁷ See the Opinion of the EDPS No. 06/2016 on *the Second EU Smart Borders Package Recommendations on the revised Proposal to establish an Entry/Exit System*, Brussels, 21.09.2016, p. 10.

⁴⁶⁸ *Ibid.*, p. 11.

⁴⁶⁹ See Article 34 of the EES Regulation whose paragraph fourth established that a period of one year is provided for family members of an EU citizens and resident with the right of free movement as initially proposed by the EU.

⁴⁷⁰ Different options were studied by the European Commission: for example, the insertion of iris recognition was discarded since its efficiency and quality were estimated to be much lower than the one given by the facial images – see the Commission Staff Working Document Impact Assessment, SWD(2016) 115 final, Brussels, 6.4.2016, p. 30.

⁴⁷¹ See Articles 22 and 27 of the EES Regulation for administrative and police purposes respectively.

‘[...] a lower number of biometric data is not necessarily synonym of a lower interference as the Proposal provides for the collection of a combination of two types of biometric data, thus allowing the use of both fingerprint matching software and facial recognition software to quickly process and sift through the data stored’⁴⁷².

In this sense, the storage of facial images was especially criticised in the EES Proposal of the European Commission, given that the same category of biometrics was already processed in the VIS. Furthermore, the simultaneous processing of different categories of biometric data – usually known as “multimodal search” – triggered EDPS’ concerns regarding the need to enhance biometric standards in order to limit error rates. Relying upon biometric data is a challenge because of the so-called FPR (False Positive Rate) and FNR (False Negative Rate) that indicate the error of accepting or rejecting a biometric claim⁴⁷³. The impossibility of capturing biometrics or comparing the biometric templates stored in the database should be also contemplated – the so-called FTC (Failure to Capture) and FTE (Failure to Enrol)⁴⁷⁴. As a consequence, measures on biometric requirements, especially for facial images, on the evaluation of biometric performance⁴⁷⁵ and on regular reporting by eu-LISA have been introduced⁴⁷⁶. These concerns also raised the fact that processing millions of pieces of data in a sole centralised system should be safeguarded with adequate security measures⁴⁷⁷. For this reason, the EDPS recommended that a new Union agency should be established as the data protection controller of the web service that enables travellers to check their application, since it is the agency the one in charge of extracting the data and putting it at the disposal of the applicant⁴⁷⁸. Needless to say, eu-LISA was assigned the development and management of the

⁴⁷² See the Opinion of the EDPS No. 06/2016 on the *Second EU Smart Borders Package Recommendations on the revised Proposal to establish an Entry/Exit System*, Brussels, 21.09.2016, p. 8.

⁴⁷³ See the ISO/IEC 2382-37:2017, Information technology — Vocabulary — Part 37: Biometrics standards, paras. 3.6.5 and 3.6.6.

⁴⁷⁴ *Ibid.*, paras. 3.9.3 and 3.9.5.

⁴⁷⁵ See the Commission Implementing Decision (EU) 2019/326 of 25 February 2019 laying down measures for entering the data in the Entry/Exit System (EES), C/2019/1210, OJ L 57, 26.2.2019, pp. 5-9, and the Commission Implementing Decision (EU) 2019/329 of 25 February 2019 laying down the specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the Entry/Exit System (EES), C/2019/1280, OJ L 57, 26.2.2019, pp. 18-28.

⁴⁷⁶ See Article 72 of the EES Regulation. This was especially emphasized by Germany in the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*, 12476/16, Brussels, 12 September 2016.

⁴⁷⁷ See the Opinion of the EDPS No. 06/2016 on the *Second EU Smart Borders Package Recommendations on the revised Proposal to establish an Entry/Exit System*, Brussels, 21.09.2016, p. 13.

⁴⁷⁸ See Article 13 of the EES Regulation – the same webpage is also used by carriers to check if a visa holder has already used its visa or not in order to allow or to refuse boarding. However, its position was not followed since data controllers shall be established by the own Member States according to Article 39 of the EES Regulation. In order to avoid cyberattacks the EDPS urged the European Commission to realise an assessment of the proportionate quantity of data that the individual should have been requested for the purposes of authentication – see the Opinion

EES, plus the duty of processing biometric data in collaboration with the Member States⁴⁷⁹. Although in the Proposal eu-LISA was also responsible for developing the National Uniform Interference (NUI), the German delegation underlined that the implementation and management of the NUI should have remained the responsibility of the national authorities⁴⁸⁰.

Biometric searches enabled the implementation of the interoperability between the EES and the VIS⁴⁸¹. This was considered as a first experiment that anticipated the legislator's Proposals on a framework for interoperability⁴⁸². On the one hand, the EES-VIS checks were indispensable in order to create an EES file for third country nationals who required a visa since identity data was retrieved from the VIS, which complied with the minimisation principle⁴⁸³. Visa-exempt third-country nationals, instead, have their biometrics registered at the borders⁴⁸⁴. On the other hand, the VIS-EES interoperability supports consulates and central visa authorities in issuing visa authorisations. The EDPS did hinder this function '[...] as long as full compliance with fundamental rights is ensured' and, in particular, the purpose limitation principle was respected⁴⁸⁵. The interoperability between EES and VIS was sealed by the implementation of a common biometric matching system that would store the biometric templates of the corresponding biometric data. Interoperability was planned for the EES project from the very beginning, as the principle of cost-effectiveness spurred the co-legislators to optimise existing architecture tools – e.g., the European Interoperability Framework (EIF)⁴⁸⁶.

of the EDPS No. 06/2016 on the *Second EU Smart Borders Package Recommendations on the revised Proposal to establish an Entry/Exit System*, Brussels, 21.09.2016, pp. 14 and 15.

⁴⁷⁹ See the amendment to Article 4 of the Council of the EU, 10880/16, Brussels, 6 July 2016, p. 8.

⁴⁸⁰ See Council of the EU, 12476/16, Brussels, 12 September 2016, pp. 17-18.

⁴⁸¹ See Article 7 of the Council of the EU, 12476/16, Brussels, 12 September 2016. The implementation of biometric searches does not replace the possibility of querying the system through alphanumeric data as established under the Commission Implementing Decision (EU) 2018/1548 of 15 October 2018 laying down measures for the establishment of the list of persons identified as overstayers in the Entry-Exit System (EES) and the procedure to make that list available to Member States, C/2018/6665, OJ L 259, 16.10.2018, pp. 39-42.

⁴⁸² See Chapter V.

⁴⁸³ The necessity to access VIS for the purposes of the EES supposes an important challenge for those Member States that still do not fully apply the Schengen *acquis*. For this purposes, Bulgaria, Romania, Croatia and Cyprus have been finally granted "passive access" to VIS only for the purposes of the EES – on the participation of these Member States to the large-scale IT systems see Chapter V.

⁴⁸⁴ See Article 15 of the Council of the EU, 12476/16, Brussels, 12 September 2016.

⁴⁸⁵ See the Opinion of the EDPS No. 06/2016 on the *Second EU Smart Borders Package Recommendations on the revised Proposal to establish an Entry/Exit System*, Brussels, 21.09.2016, p. 15.

⁴⁸⁶ See the study of the European Commission, *New European Interoperability Framework: Promoting seamless services and data flows for European public administrations*, Brussels, 2017. Also confront the position assumed by Estonia in the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*, 8701/16, Brussels, 12 May 2016. The Estonian delegation also stand out that opting for a centralised system, instead of a decentralised one, the legislator was opting for a less secure infrastructure subjected to cyberattacks.

Finally, a second Proposal was presented by the European Commission to facilitate the speeding up of crossing of borders by so-called *bona fide* travellers. Thus, and despite the fact that the European Commission announced the withdrawal of the RTP, the European Commission's impact assessment indicates that the RTP was still in the air. The RTP project proposed in 2013 contemplated a procedure very close to the one set forth in the Visa Code for visa applicants: travellers that registered in the RTP database could pass through the eGates established for EU citizens⁴⁸⁷. Instead of definitively abandoning this project, the European Commission evaluated two further options to facilitate border crossings. In the first option, the applicant should have been registered in the EES or the VIS and would have submitted a request and the relevant documents via the website with the payment of a fee. At the borders, the RTP process would have been activated. With this solution, the EES and the RTP would not be merged in a unique database, which reduced the 'project management risk'⁴⁸⁸. The second option would have allowed the establishment of a unique database through a 'process accelerator'. This means that the traveller would have been subjected to a risk assessment using the information provided at the border crossing points, the responses from the various consulted databases – including the EES – and the answers provided by the travellers through self-service systems. Such a mechanism would have enabled the border guards to decide not to ask the traveller additional questions when a "face to face" border check was not necessary, and it would have avoided the implementation of a new system. To achieve this, self-service systems⁴⁸⁹, e-Gates⁴⁹⁰ and automated border control systems⁴⁹¹ were to be implemented. In addition, Member States could have still established national facilitation programs that reduced the number of checks at the external borders⁴⁹². In the end, the second Proposal was adopted with a separate initiative on the usage of EES that amended the Schengen Borders Code.

⁴⁸⁷ Concretely, and although border checks still would be applicable, the RTP program would have avoided questions on: scrutiny of the travel document for signs of falsification or counterfeiting; the point of departure/destination, the purpose of intended stay, and the means of subsistence – see the Commission Staff Working Document Impact Assessment, SWD(2016) 115 final, Brussels, 6.4.2016.

⁴⁸⁸ According to the Commission Staff Working Document Impact Assessment, *ibid.*, p. 26:

'Project management risk refers to the likelihood that a project does not deliver the IT services that are within the remit of the project with the required quality and performance, on time and within budget. So, the main risks of a project are that the project either fails to deliver all the IT services, whether it fails on the quality or performance of these services and whether the project is completed on time and without significant budget overruns. The view is that a "small" project carries a lower risk than a "large" project'.

⁴⁸⁹ According to Article 1(1) of EES Regulation, "self-service system" means an automated system which performs all or some of the border checks that are applicable to a person and which may be used for pre-enrolling data in the EES.

⁴⁹⁰ According to Article 1(1) of EES Regulation, "e-gate" means an infrastructure operated by electronic means where an external border or an internal border where controls have not yet been lifted is actually crossed.

⁴⁹¹ According to Article 1(1) of EES Regulation, "automated border control system" means a system which allows for an automated border crossing, and which is composed of a self-service system and an e-gate.

⁴⁹² See under Article 1 of the EES Regulation.

6. European Travel Information and Authorisation System (ETIAS)

In its Communication of 2008⁴⁹³, the European Commission advanced the idea that an Electronic Travel Authorisation System (ESTA)⁴⁹⁴ would be introduced. Although the ETIAS did not accompany the EES and the RPT Proposals of 2013, the European Commission renewed its engagement with this project in 2016's Security Strategy on Stronger and Smarter Information Systems for Borders and Security when the EES revised legislative Proposal was also announced. Furthermore, the European Commission jumped to the revised EES Proposal so as to develop the ETIAS architecture: these systems share the same hardware and software and the same identity repository – i.e., the same “container” of identity data⁴⁹⁵ – however, the ETIAS does not contain biometrics.

The ETIAS Proposal⁴⁹⁶ forms part of the EU Integrated Border Management Strategy and it is underpinned by Article 77(2)(d) TFEU as a tool to determine whether visa-exempt third country nationals⁴⁹⁷ represent a risk to security, irregular migration, or high epidemic before their arrival at the EU external borders⁴⁹⁸. In this sense, ETIAS' contribution goes beyond “physical borders” to manage migration flows and threats to national security and public order in third countries⁴⁹⁹. Indeed, the ETIAS application form is filled-in by the applicants themselves in the third country and it is processed as described hereafter.

⁴⁹³ See the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2008) 0069 final, Brussels, 13.2.2008, paras. 2, 3 and 4.

⁴⁹⁴ The Policy study on the EU Electronic System for travel Authorisation (EU ESTA) of February 2011 is available at www.ec.europa.eu.

⁴⁹⁵ Only the entry and exit records are separately stored and linked to the correspondent EES identification file.

⁴⁹⁶ See the Proposal for a Regulation of the European Parliament and the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624, COM(2016) 0731 final, Brussels, 16.11.2016.

⁴⁹⁷ Among them, family members of EU citizens and those that benefit from the right to free movement are included. However, though the latter group is recognised the right to enter the EU and, as such, it shall be facilitated the issuing of the authorization without any charge. Furthermore, both groups are only assessed whether they constitute a security threat, but not the risk of irregular staying in the territory of the Member State – see recitals (6) to (8) of the ETIAS Regulation.

⁴⁹⁸ In general terms, ETIAS' purposes were found to be too vague so as to assess the proportionality of this legislative measure and the EDPS urged to the European Commission to better define which the parameters relevant to evaluate the migration and security risks. As a consequence, “security risk”, “illegal immigration risk” and high “epidemic risk” have been concretised in the body of the act – see Article 3(6), (7) and (8) respectively of ETIAS Regulation.

⁴⁹⁹ See the Opinion of the Article 29 DPWP in the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*, 8231/17, Brussels, 12 April 2017.

Following the experiences of overseas countries such as the US, Canada, and Australia⁵⁰⁰, the ETIAS was presented as the most efficient solution for both border guards and travellers and a means of reducing the number of refusals of entry at the external borders. In this sense, the system is directed at strengthening the controls at land borders⁵⁰¹, while travellers by air or sea already feed national databases with personal information through the API and/or the PNR instruments – being the latter only being valid for air arrivals. This implies that the ETIAS Regulation is underpinned by another legal basis, that is Article 77(2)(b) TFEU⁵⁰².

Being that the data manually inserted via the web or a mobile application⁵⁰³, up to now the ETIAS is the sole large-scale IT system storing alphanumeric data alone – namely identity data and travel document data⁵⁰⁴. Despite the lack of biometrics, the huge amount of data stored in the ETIAS was found to be disproportional, both by the EDPS⁵⁰⁵ and the Article 29 DPWP⁵⁰⁶, as some categories of data stored therein are not required to visa applicants – e.g., their education level or their current occupation. The same position was assumed by the European Parliament that suggested deleting some superfluous data after the crossing of external borders, and to rely on the assessments provided by the European Centre for Disease Prevention and Control and disease outbreaks reported by the World Health Organisation regarding health

⁵⁰⁰ During the negotiations it was advanced the possibility that in case the travel authorisation would have been automatically refused, the person should have been requested a visa to entry the Schengen area which resembled the US Electronic System for Travelling Authorization (ESTA) under the so-called Visa Waiver Program (similarly, Canada and Australia adopted the eTA and eVisitor Programme). However, this possibility was dropped by the Legal Service of the EU Council since it would have implied a radical change in the EU visa policy – see the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS)*, 6324/17, Brussels, 20 February 2017, p. 2. Furthermore, a huge debate arose with regard to the airports' transit zones. At the beginning, the delegations supported that both visa and visa exempt third country nationals should have been in possession of a travel authorization, unless they require a transit visa or possess a valid visa. However, this position did not pass the European Parliament's scrutiny as stated in the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*, 15127/17, Brussels, 15 December 2017, p. 2.

⁵⁰¹ Confront the Proposal for a Regulation of the European Parliament and the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations, (EU) No. 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624, COM(2016) 0731 final, Brussels, 16.11.2016, pp. 4 and 5.

⁵⁰² See recital (11) of the ETIAS Regulation.

⁵⁰³ See the Commission Delegated Decision (EU) 2019/971 of 26 February 2019 on the definition of the requirements of the secure account service pursuant to Article 6(4) of Regulation (EU) 2018/1240 of the European Parliament and of the Council, enabling applicants to provide any additional information or documentation required (Text with EEA relevance), C(2019)1695, OJ L 156, 13.6.2019, pp. 20-24, and, in case of withdrawal of the application, the Commission Delegated Decision (EU) 2019/969 of 22 February 2019 on the tool enabling applicants to give or withdraw their consent for an additional retention period of their application file pursuant to Article 54(2) of Regulation (EU) 2018/1240 of the European Parliament and of the Council (Text with EEA relevance), C(2019)1532, OJ L 156, 13.6.2019, pp. 10-14.

⁵⁰⁴ See Article 17(2), (3) and (4) of the ETIAS Regulation.

⁵⁰⁵ See the Opinion of the EDPS No. 3/2017 on the *Proposal for a European Travel Information and Authorization System (ETIAS)*, Brussels, 6 March 2017, p. 17.

⁵⁰⁶ See the Opinion of the Article 29 DPWP in the Council of the EU, 8231/17, Brussels, 12 April 2017.

information⁵⁰⁷. In addition, the European Parliament dictated that residential address information should be inserted on a voluntary basis⁵⁰⁸. The European Commission also refused the insertion of other categories of data requested by the delegations in the EU Council, including the purpose of the visit, the traveller's means of subsistence, and the duration of the first intended stay⁵⁰⁹, and it warned that the necessity and proportionality principles could be challenged before the CJEU⁵¹⁰. Although the ETIAS Regulation specifies that the issuance of a travel authorisation differs from visa policy, based on the negotiations a confrontation between the two systems seems to be unavoidable. The debate on the supposed "equal treatment" of visa applicants and those who do not require visas gave rise to a strange formulation in the ETIAS Regulation (9) that states that: on one hand the nature of a travel authorisation differs from that of a visa and, on the other hand, that the ETIAS consists of a new entry condition for which no additional information may be requested than that required from visa applicants⁵¹¹.

The quantity and quality of the data processed by the ETIAS shall be justified in light of the new risk-based approach and algorithm technology that was used as part of the experiment. The process was established to calculate the risk to security, of irregular migration, or the chances of spreading disease, in an automated manner, and it is launched by the applicants themselves as soon as they complete the online application⁵¹². Once the travel authorisation request is launched⁵¹³, the data is cross-matched in different ways: first, with the large-scale IT systems records and the Interpol databases; second, with an ETIAS Watchlist and, finally, with a set of screening rules.

⁵⁰⁷ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*, 13907/17, Brussels, 17 November 2017, p. 3.

⁵⁰⁸ See the Council of the EU, 15127/17, Brussels, 15 December 2017.

⁵⁰⁹ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*, 9349/17, Brussels, 19 May 2017, p. 3.

⁵¹⁰ *Ibid.*, p. 3.

⁵¹¹ Recital (9) of the ETIAS Regulation: '[...] As such, a travel authorisation is by its nature distinct from a visa; it will not require more information or place a heavier burden on applicants than a visa does. Holding a valid travel authorisation should be a new entry condition for the territory of the Member States. Mere possession of a travel authorisation should not, however, confer an automatic right of entry'.

⁵¹² The travel authorisation is requested for applicants between eighteen and seventy years old and it costs seven euros according to Articles 18 of the ETIAS Regulation.

⁵¹³ See Article 19 of the ETIAS Regulation that establishes that the application is admissible when the application contains all the items referred to in Article 17(2), the answers to the question established in Article 17(4) of the ETIAS Regulation, and the travel authorisation fee has been collected.

In the first stage, the data is extracted from the application and cross-matched against the ETIAS records⁵¹⁴ and the other systems, namely: the SIS⁵¹⁵; the VIS⁵¹⁶; the EES⁵¹⁷; the Eurodac⁵¹⁸; the Europol data⁵¹⁹, and the Interpol databases SLTD and TDAWN⁵²⁰. The interoperability between the ETIAS and the other large-scale IT systems, as well as Europol data and Interpol databases, raised huge concerns with regard to the right to the protection of personal data. The EDPS called for an assessment of the compatibility of the purposes of the cross-matched systems⁵²¹ since each database was designed to pursue its own objectives and these may not be compatible with those sought by ETIAS, or vice versa. In its Opinion, the EDPS added that the underlying legal bases underpinning the system may need to be enlarged because of the additional goals brought in by the ETIAS' automated checks⁵²².

The ETIAS' interoperability with the other systems, data, and databases was one of the most sensitive issues touched upon during the negotiations and in the negotiations on the later amendments to the ETIAS⁵²³. Again, the later amendments to the ETIAS are split into two

⁵¹⁴ Article 19(4) of the ETIAS Regulation establishes that ETIAS data shall reveal if: any other valid travel authorisation exists; the data provided in the application concerning the travel document corresponds to another application for travel authorisation associated with different identity data, and the applicant or the associated travel document do not correspond to a refused, revoked, or annulled application for travel authorisation.

⁵¹⁵ As for the SIS II, the ETIAS checks shall verify whether the applicant is subject to an alert on refusal of entry, on European Arrest Warrant or on wanted for arrest for extradition purposes, as well as if the travel document is reported as lost, stolen or invalidated is verified through SIS and the Interpol TDAWN – see Article 20(2)(a), (c) and (d) of the ETIAS Regulation. In case of minors, the SIS II is checked to assess if the applicant's parental authority or legal guardian is subject to an alert in respect of persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes in the SIS II or is subject to a refusal of entry and stay alert entered in the SIS II – see Article 20(2)(m) of the ETIAS Regulation.

⁵¹⁶ If the applicant was granted visa waiver status within five years or less, or s/he as more than one nationality, the VIS is hit to see if in the previous status of visa third country national the applicant was refused a visa application – see Article 20(2)(i) of the ETIAS Regulation.

⁵¹⁷ The EES is consulted to see if the applicant has been recorded as an overstayers or he was refused to entry – see Article 20(2)(g) and (h) of the ETIAS Regulation.

⁵¹⁸ See Article 20(2)(k). The new Eurodac is expected to enable the calculation of the risk of irregular migration by taking into account if the applicant was subject to a return decision or a removal order issued following the withdrawal or rejection of the application for international protection. However, the binomen ETIAS-Eurodac has been set apart from the moment since the Eurodac negotiations are still ongoing and currently this database does not store alphanumeric data but only biometrics.

⁵¹⁹ See Article 20(2)(j) of the ETIAS Regulation.

⁵²⁰ See Article 12 of the ETIAS Regulation that wants to assess if the travel document is reported as lost, stolen or invalidated (SLTD) and/or his/her travel document are subject to an Interpol alert (TDAWN).

⁵²¹ See the Opinion of the EDPS No. 3/2017 on *the Proposal for a European Travel Information and Authorization System (ETIAS)*, Brussels, 6 March 2017, p. 17.

⁵²² The European Union Fundamental Rights Agency (FRA) stand out that the exercise of the right to access, corrections and erasure data shall be granted also when the information “originates from other systems” and the applicant shall receive clear information on how to exercise subjective rights – see the Opinion of the FRA No. 2/2017, *The impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorization System (ETIAS)*, Vienna, 30.06.2017.

⁵²³ See Article 11(2) of the ETIAS Regulation and: Regulation (EU) 2021/1151 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EU) 2019/816 and (EU) 2019/818 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the European Travel Information and Authorisation System, PE/16/2021/REV/1, OJ L 249, 14.7.2021, pp. 7-14, and Regulation (EU) 2021/1152 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EU)

Regulations since: a first Proposal was submitted concerning the ETIAS checks with the ECRIS-TCN⁵²⁴ and the SIS II for law enforcement purposes⁵²⁵; a second one, instead focused on the interoperability of the ETIAS with the EES, the VIS, and the SIS II on border issues⁵²⁶. The EDPS specifically focused on the interconnection between the ETIAS and the ECRIS-TCN and noted that the interoperability between these two systems adds to the latter a new purpose of consultation for border management issues, and allows the access of new authorities, namely the ETIAS Central Unit and the ETIAS National Units⁵²⁷. In their words:

‘The EDPS recalls that the ECRIS-TCN aims at enhancing judicial cooperation in criminal matters by improving the exchange of information on criminal records through the EU. Using the data stored in the ECRIS-TCN for border management purposes would go far beyond the purposes of the ECRIS-TCN defined in its constitutive legal instrument (as currently agreed). Instead, this would be an example of what is often described as “function creep”, namely, a gradual widening of the use of a system or database beyond the purpose for which it was originally intended’⁵²⁸.

For their part, the Member States’ delegations were especially concerned by the fact that only terrorism and other serious criminal offences were relevant to the purpose of ETIAS but, as we will see in the next paragraph, the ECRIS-TCN does not anticipate any differentiation between different categories of criminal offences⁵²⁹.

In addition, the EES-ETIAS interoperability has been revised so that it is limited to cases where the EES cross-matches with ETIAS while performing individual checks at the EU

2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861 and (EU) 2019/817 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the European Travel Information and Authorisation System, PE/17/2021/REV/1, *OJL* 249, 14.7.2021, pp. 15-37.

⁵²⁴ The ECRIS-TCN is consulted to see if the applicant has been convicted in one of the Member States as we will explain in the next paragraph.

⁵²⁵ See the Proposal for a Regulation of the European Parliament and of the Council establishing the conditions for accessing the other EU information systems and amending Regulation (EU) 2018/1862 and Regulation (EU) yyyy/xxx [ECRIS-TCN], COM(2019) 3 final, Brussels, 7.1.2019, on the basis of Article 87(2)(a) and Article 82(1)(d) TFEU respectively. It shall be underlined that as for the SIS II alerts on persons wanted for arrest for surrender purposes or extradition purposes or to an alert on persons for discreet checks or specific checks should not prevent them from being issued with a travel authorization. This would enable Member States to take appropriate action in accordance with Council Decision 2007/533/JHA – see recital (13) of the ETIAS Regulation.

⁵²⁶ See the Proposal for a Regulation of the European Parliament and of the Council establishing the conditions for accessing other EU information systems for ETIAS purposes and amending Regulation (EU) 2018/1240, Regulation (EC) No 767/2008, Regulation (EU) 2017/2226 and Regulation (EU) 2018/1861, Brussels, 7.1.2019. The SIS II return alerts were discarded since they are deleted once the individual is returned to the third country. Being the European travel authorisation requested only from outside the Schengen area, by definition the applicant cannot have a pending return alert.

⁵²⁷ See Articles 22 and 26 of the ETIAS Regulation.

⁵²⁸ See the letter sent by Giovanni Buttarelli to the delegations in Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing the conditions for accessing other EU information systems for ETIAS purposes and amending Regulation (EU) 2018/1240, Regulation (EC) No 767/2008, Regulation (EU) 2017/2226 and Regulation (EU) 2018/1861* Proposal for a Regulation of the European Parliament and of the Council establishing the conditions for accessing the other EU information systems and amending Regulation (EU) 2018/1862 and Regulation (EU) yyyy/xxx [ECRIS-TCN] *Comments of the European Data Protection Supervisor*, 7553/19, Brussels, 15 March 2019, p. 3.

⁵²⁹ See the Council of the EU, 13907/17, Brussels, 17 November 2017, p. 7.

external borders⁵³⁰. In order to use the system, border guards have been also granted the right to access some data from the ETIAS files⁵³¹ and the EDPS recalled, once more, the need to conduct a relevant impact assessment together with the European Commission proposal in order to evaluate the effects of the proposal on the fundamental rights of individuals. The fact that no impact assessment was conducted either for the ETIAS Proposal or for the ETIAS' consequential amendments is consolidating bad practice within the European Commission in the field of IT systems. The latter was justified on the basis of the fact that consequential amendments would only require technical changes; yet, their impact on the protection of individual's rights was strongly debated during the political discussions. It is hoped that the European Commission's Communication Better Regulation⁵³² that proposes to streamline consultation procedures and strengthen impact assessment proceedings will mark a change of course in the Commission's favour⁵³³.

In any case, as we were advancing, the data inserted in the application is confronted against the ETIAS Watchlist stored in the ETIAS Central System⁵³⁴. The ETIAS Watchlist was created by Europol to gather the data related to persons who are suspected of having committed, or having taken part in a criminal offence, who have been convicted of such an offence, or about whom there are factual indications or reasonable grounds to believe that they will commit such an offence⁵³⁵. The Watchlist is fed by the information stored by Europol and the Member States, and it is hosted by eu-LISA⁵³⁶. However, given that Europol's mandate falls outside the scope of the Schengen *acquis*⁵³⁷, its participation in the ETIAS has been regulated by a separate legislative act⁵³⁸ underpinned by Article 88(2)(a) TFEU.

Finally, in a third final step, the ETIAS applies a set of screening rules through the use of an algorithm that compares the data recorded in the ETIAS application file against a set of "risk criteria" with the aim of predicting the risk of irregular migration, or to security, or public

⁵³⁰ During border checks, the ETIAS Central System is checked by reading travel document's machine-readable zone or application number – see Article 47(1) of the ETIAS Regulation.

⁵³¹ See Article 47 of the ETIAS Regulation.

⁵³² Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Better regulation: Joining forces to make better laws, COM(2021) 219 final, Brussels, 29.4.2021.

⁵³³ See the "Mieux légiférer", les États membres soutiennent globalement l'approche 'One in, one out'", *Bulletin Quotidien Europe*, No. 12802, 1.10.2021.

⁵³⁴ See Article 20(4) of the ETIAS Regulation.

⁵³⁵ See Article 34(3) of ETIAS Regulation.

⁵³⁶ See Article 35 of the ETIAS Regulation.

⁵³⁷ Remembering that the Schengen Associated Countries do not participate in Europol as we will explain in Chapter V.

⁵³⁸ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*, 10017/17 ADD 1, Brussels, 13 June 2017.

health⁵³⁹. The use of algorithm technology implements a profiling technique that raised serious concerns with regard to the principle of no discrimination⁵⁴⁰. Although the ETIAS excludes the processing of sensitive data like race, ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, sex life or sexual orientation⁵⁴¹, the EDPS and the Article 29 DPWP underlined that this is not sufficient, as other types of information may indirectly uncover such data – including nationality, the country and city of residence of an applicant, their sex and current occupation. Moreover, the necessity of such a questionable technique was not adequately justified as the automated checks executed by the ETIAS may have been considered sufficient to prevent risks to security, migration, and health. Despite this, screening rules have been maintained as part of the ETIAS’ automated procedure; yet, upon the European Parliament initiative, an ETIAS Fundamental Rights Guidance Board was set up to ensure the respect of fundamental rights while applying the ETIAS screening rules and risk indicators⁵⁴².

Once the automated processing ends, and if no hit is detected, the travel authorisation is automatically issued⁵⁴³. However, if some hits occur, the competent authority in charge of verifying whether the data matched corresponds to the same person or not is the ETIAS Central Unit⁵⁴⁴ – or the SIRENE Bureau in the specific case of “sensitive alerts” on missing persons, on persons sought to assist with a judicial procedure and on persons requiring discreet checks or specific checks⁵⁴⁵. The ETIAS Central Unit was established within the EBCG Agency and is accompanied by the ETIAS Screening Board⁵⁴⁶ that manages the ETIAS Watchlist and supports the ETIAS Central Unit in establishing the risks indicators that enable the screening procedure⁵⁴⁷ on the basis of previously correlated statistics⁵⁴⁸.

For the purposes of verification, the ETIAS Central Unit shall have access to the application file and any linked application files already stored in ETIAS, as well as to all hits triggered

⁵³⁹ See Article 33 of the ETIAS Regulation.

⁵⁴⁰ See the Opinion of the EDPS No. 3/2017 on the *Proposal for a European Travel Information and Authorization System (ETIAS)*, Brussels, 6.03.2017, and the Opinion of the Article 29 DPWP in Council of the EU, 8231/17, Brussels, 12 April 2017.

⁵⁴¹ See recital (27) of the ETIAS Regulation.

⁵⁴² Article 10 of the ETIAS Regulation establishes the composition of the ETIAS Fundamental Rights Guidance Board as follows: a Fundamental Rights Officer of the EBCG Agency; a representative of the consultative forum on fundamental rights of the EBCG Agency; a representative of the EDPS; a representative of the EDPB established by the GDPR, and a representative of the FRA.

⁵⁴³ See Article 21(1) of the ETIAS Regulation.

⁵⁴⁴ See Article 20 of the ETIAS Regulation. On the preparation of the ETIAS Central Unit, see the Council of the EU, *Frontex report on the ETIAS state of preparation*, 7336/20, Brussels, 15 April 2020.

⁵⁴⁵ See recital (12) of the ETIAS Regulation.

⁵⁴⁶ The ETIAS Screening Board will be composed by each ETIAS National Unit and Europol – see Article 9 of the ETIAS Regulation.

⁵⁴⁷ See Article 7(2)(c) of the ETIAS Regulation.

⁵⁴⁸ See Article 33(2) of the ETIAS Regulation.

during the automated processing and to the information identified by the ETIAS Central System. The purpose is to individualise whether a Member State or Europol⁵⁴⁹ has entered or supplied the data responsible for triggering the hit⁵⁵⁰. This implies that the ETIAS Central Unit has access not only to the other requests that the applicant may have previously forwarded, but also to the identity data related to the applicant that is stored in the underlying systems, albeit temporarily⁵⁵¹.

If the ETIAS Central Unit confirms that the automated processing has resulted in a hit, or there are doubts about the identity of the applicant, it will transfer the application and accompanying information to the ETIAS National Unit⁵⁵² of the Member State “responsible” for the manual processing⁵⁵³. The ETIAS National Unit is also in charge of manually processing the applications and of issuing, or not, the travel authorisation when a hit is reported with regard to the set of questions that the applicant was asked in the application form⁵⁵⁴. For this purpose, the ETIAS National Unit can access the application file and any linked application file stored in ETIAS, as well as any hits triggered during the automated processing. The amendments to the ETIAS also give the ETIAS National Unit direct access to the relevant identity files – previously retrieved by the ETIAS Central Unit – that are stored in the underlying IT systems⁵⁵⁵. Unlike the ETIAS Central Unit, the ETIAS National Unit can also ask for additional information and documentation and, in exceptional cases, the applicant may be invited to an interview in the consulate of the country of their residence⁵⁵⁶. For these purposes, the ETIAS National Unit can consult the information available in other databases and decentralised systems, while Member States and Europol⁵⁵⁷ can be contacted when they are responsible of having triggered the hit⁵⁵⁸.

If the travel authorisation is finally issued, it enables multiple entries to the Schengen area for five years⁵⁵⁹. The EDPS questioned the standard retention period, which was also adopted for the EES and the VIS, and asked the European Commission to provide specific periods

⁵⁴⁹ In case the hit is triggered against Europol data, it will be forwarded the application file, any linked ETIAS file, and the relevant data by the ETIAS Central Unit. The information shall be forwarded through the ETIAS software.

⁵⁵⁰ See Article 22 of the ETIAS Regulation.

⁵⁵¹ See Article 11(8) of Regulation (EU) 2021/1152.

⁵⁵² See Article 7(2)(f) of the ETIAS Regulation.

⁵⁵³ See Article 25 of the ETIAS Regulation.

⁵⁵⁴ See Article 21(3) and (4) of the ETIAS Regulation that recalls its Article 26.

⁵⁵⁵ See Article 25a of Regulation (EU) 2021/1152.

⁵⁵⁶ See Article 27(4) of the ETIAS Regulation.

⁵⁵⁷ In this case the proceeding described under Article 29 of the ETIAS Regulation applies. The provision does not give Europol the access to the system, but the information should be transferred to it.

⁵⁵⁸ See Article 26(1) of the ETIAS Regulation.

⁵⁵⁹ During the negotiations, it was contemplated the option or reduce the period to up two years as it is regulated in the US ESTA program. See the Council of the EU, 6324/17, Brussels, 20 February 2017, p. 5.

according to each category of data⁵⁶⁰. This may be particularly relevant for health data that, as the EDPS notes, constitutes a category of sensitive data that is not stored in any other large-scale IT system. As part of the same opinion, the EDPS underlined that the time limit for storing health data may not be reliable as it would not necessarily reflect the current status of the applicant. On the contrary, it welcomed the European Commission provision that forbade law enforcement authorities and Europol to access health data.

If it is issued, the travel authorisation may be “flagged” by the ETIAS National Unit in order to warn the border guard authority of the need to further examine the application before granting the access to the territory – so-called second line checks⁵⁶¹. In any case, the travel authorisation does not give the right to enter the Schengen territory as the last word is left to the border guards⁵⁶². Indeed, border guard authorities still maintain their competence to check the prerequisites of entry at the borders and the ETIAS is supposed to facilitate their job. In this sense, carriers are also given access to the ETIAS to check whether the individual holds the required travel authorisation to embark on an aircraft or vessel⁵⁶³.

If the authorisation is not issued⁵⁶⁴, the ETIAS Regulation specifies that the applicant has the right to appeal the decision in the Member State that has taken the decision and in accordance with its national law⁵⁶⁵. This point was especially debated during the negotiations,

⁵⁶⁰ See the Opinion of the EDPS No. 3/2017 on *the Proposal for a European Travel Information and Authorization System (ETIAS)*, Brussels, 6.03.2017, p. 17.

⁵⁶¹ See Article 36(2) of the ETIAS Regulation and the Commission delegated decision of 10.12.2020 supplementing Regulation (EU) 2018/1240 of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) as regards flagging, COM(2020) 8709 final, Brussels, 10.12.2020.

⁵⁶² See recital (9) *in fine* of the ETIAS Regulation.

⁵⁶³ See Article 45 of the ETIAS Regulation. ETIAS is consulted by reading the travel document’s machine-readable zone or inserting the application number. Carriers are liable to take the traveler back and incurs in a penalty in case they transport an individual without the travel authorisation. The FRA underlined that in no case this obligation shall prejudice the right to seek asylum and urged the insertion of a specific provision on this aspect. On the contrary, it welcomed the provision that enabled visa exempt third country nationals to apply for a travel authorisation with a limited territorial and temporal validity – see the Opinion of the FRA No. 2/2017, *The impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorization System (ETIAS)*, Vienna, 30.06.2017. It shall be noted that the European Parliament proposed to reduce the burdens endorsed to carriers by establishing a transitional period where no obligation of return should be imposed and, after that, a reduction of the penalty should apply as well – see the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*, 7152/18, Brussels, 22 March 2018, p. 3. This is now reflected in Article 45(9) of the ETIAS Regulation.

⁵⁶⁴ In case of refusal, revocation, or annulment, as well as when the applicant gives to consent to have his/her ETIAS application file stored after the expiration period, the applicant has the right to see the status of the application through the verification tool established by Commission Delegated Decision (EU) 2019/970 of 22 February 2019 on the tool for applicants to check the status of their applications and to check the period of validity and status of their travel authorisations pursuant to Article 31 of Regulation (EU) 2018/1240 of the European Parliament and of the Council (Text with EEA relevance), C(2019)1533, OJ L 156, 13.6.2019, pp. 15-19.

⁵⁶⁵ During the negotiations, it was also advanced the possibility that the Member State of intended stay (and not first entry) should have been responsible of issuing or refusing the authorisation in order to not overcharging large airports or with a land border. Moreover, when the refusal of the authorisation would have depended on an alert

as Member States were undecided on whether to allocate the responsibility to the Member State of first entry or to Member State at the origin of an alert triggering a “hit”⁵⁶⁶. The FRA recalled that in the light of Article 47 of the CFREU, Member States shall ensure that the applicant has the decision judicially reviewed since administrative instances or non-judicial reviews are not sufficient to guarantee this right⁵⁶⁷. It therefore invited the European Commission to insert further details regarding the reasons for refusal in order to allow the applicant to appeal the decision⁵⁶⁸. Whether positive or not, the final decision shall be evaluated within seven working days, though no deadline is provided for the issuing of the final decision⁵⁶⁹.

Despite the fact that the ETIAS aims at supporting three different EU policies – namely security, illegal migration, and public health – these purposes do not stand on an equal footing. From the very beginning, the European Commission admitted that the rate of visa-exempt irregular migration is relatively low, but there was a “need” to cover the information gaps existing with respect to irregular migrants as they may represent a security risk⁵⁷⁰. Security is also the main justification regarding the restriction of fundamental rights caused by the ETIAS Proposal in light of the right to the protection of personal data and the limits to its restriction set forth under Article 52 of the CFREU⁵⁷¹. Indeed, and as the EDPS underlined, the ETIAS information is available to Europol and law enforcement authorities for the purposes of prevention, detection, or investigation of a terrorist offence, or other serious criminal offences⁵⁷².

The EDPS has included the ETIAS Proposal in the legislative trend of combining migration management and security in the field of IT systems, which, in its opinion, includes: the granting of access to databases intended for other purposes to law enforcement authorities; the

inserted by another Member State, delegations were wondering whether that Member State should have been responsible instead – see the Council of the EU, 6324/17, Brussels, 20 February 2017, pp. 3 and 4, and the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*, 6929/17, Brussels, 8 March 2017.

⁵⁶⁶ See, among others, the Council of the EU, *Information Technology (IT) measures related to border management a) Entry/Exit System (EES) b) EU Travel Information and Authorisation System (ETIAS) = Progress report*, 7064/17, 17 March 2017, p. 3 and the *European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624. - the issue of the Member State responsible for manual processing of applications*, 7554/17, Brussels, 23 March 2017.

⁵⁶⁷ Recalling that the same statement was made as for visa short stay the in Council of the EU, *2014 Report on the Application of the EU Charter of Fundamental Rights*, COM(2015) 191, Brussels, 8 May 2015, pp. 7-8.

⁵⁶⁸ The same considerations shall be valid as for annulment and revocation of the authorisation.

⁵⁶⁹ See recital (42) *in fine* of the ETIAS Regulation.

⁵⁷⁰ See Article 7(2)(b) of the ETIAS Regulation.

⁵⁷¹ *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No. 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*, 2016/0357 (COD), 16.11.2016, pp. 19-21, Brussels, 16.11.2016.

⁵⁷² Note that the request of Europol is processed by the ETIAS Central Unit according to Article 7(2)(j) of the ETIAS Regulation.

establishment of new information systems, and the extension of the competences of the existing body⁵⁷³. The expansion of ETIAS' scope to law enforcement also justifies its roots in Article 87(2)(a) TFEU⁵⁷⁴. Along the same lines, Europol can ask to access the ETIAS information for the purpose of preventing, detecting, or investigating terrorist offences or other serious criminal offences⁵⁷⁵. Both law enforcement authorities' and Europol's access to ETIAS has been limited to a cascade approach for which national databases and the Europol data shall be consulted before accessing the ETIAS. Furthermore, access by law enforcement and Europol shall first be reviewed by the Central Access Point, except in cases of extreme urgency⁵⁷⁶. Yet, the EDPS doubted the necessity to access the ETIAS for these purposes as the same set of data is processed in the EES, database to which these bodies have been granted access rights.

All in all, and although the ETIAS' balance seems to tip toward the security aspect, it cannot be ignored that other interests also benefit from the system. Indeed, the ETIAS can be also accessed by immigration authorities which caused issues with the European Parliament until a cascade approach was agreed⁵⁷⁷. The ability of migration authorities to access the system opens the door to another debate that concerns the transfer of data to third countries for the purposes of return and that was agreed under the same logic by which previous checks in the EES database are mandatory⁵⁷⁸. According to the EDPS:

⁵⁷³ See Opinion of the EDPS No. 3/2017 on *the Proposal for a European Travel Information and Authorization System (ETIAS)*, Brussels, 6 March 2017, p. 8.

⁵⁷⁴ See Chapter X of the ETIAS Regulation.

⁵⁷⁵ See Article 53 of the ETIAS Regulation and the Council of the EU: *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorization System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*, 8584/17, Brussels, 10 May 2017, and *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624 - Information of the European Parliament on the splitting of the original proposal into two texts*, 10364/17, Brussels, 23 June 2017. The amendments to the Europol Regulation were agreed on the basis of the interinstitutional dialogues among the legislators that avoided the second reading and conciliation according to the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS) – Outcome of the European Parliament's first reading (Strasbourg 2 to 5 July 2018)*, 10545/18, Brussels, 12 July 2018. They were finally adopted in September 2018 by Regulation (EU) 2018/1241 of the European Parliament and of the Council of 12 September 2018 amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS), *OJ L* 236, 19.9.2018, p. 72.

⁵⁷⁶ See recitals (42) to (46). Yet, during the negotiations the supervision was endorsed to a court or an independent authority and the EDPS pushed for its insertion in the body of the text (Article 45) and recommended to designate the national supervisory authorities responsible to verify the access rights – see the Opinion of the EDPS No. 3/2017 on *the Proposal for a European Travel Information and Authorization System (ETIAS)*, Brussels, 6.03.2017, p. 18 ff. In the final text, the Central Access Point is regulated under Articles 50 and 53 for law enforcement authorities and Europol respectively.

⁵⁷⁷ See recital (39) and Article 49 of the ETIAS Regulation for which for which the authorities have the obligation to first consult the EES, and only if the third country national is not registered in the EES, the immigration authorities may access some ETIAS data.

⁵⁷⁸ See Chapter VI.

‘[t]his has an impact in terms of data protection since more personal data will be collected and be accessed by various authorities (immigration authorities, border guards, law enforcement authorities, etc.)’.

The EDPS stressed that, although migration and internal security might converge, these are two different public policies with distinct objectives and key actors.

By way of conclusion, we cannot avoid pointing out that the ETIAS crucially contributes to the implementation of the IO Regulations. The automated checks performed by the Central System pave the way toward the elaboration of one of the interoperability components that will be analysed in Chapter V, that is, the ESP.

7. European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN)

The ECRIS-TCN was established following the creation of the European Information System on Criminal Records (ECRIS)⁵⁷⁹. The ECRIS is a decentralised database that has been in operation since 27 April 2012 and that allows the interconnection of Member States’ national databases for the purpose of cooperation in criminal proceedings – and, if permitted by national law, for other purposes including administrative procedures, background checks by employers, and the issuing of licenses⁵⁸⁰. The ECRIS was born as a tool designed to support Council Framework Decision 2008/675/JHA for which Member States shall take into consideration the convictions imposed by another Member State within a criminal proceeding⁵⁸¹.

In the ECRIS architecture, a Member State keeps the criminal records of their own convicted nationals, including the sentence imposed by the Member State of which the individual is a national, or by another Member State. Therefore, the ECRIS does not confer the right to directly access the information held by another Member State⁵⁸² but establishes a network among the Member States’ Central Authorities that are in charge of exchanging the information⁵⁸³. This may consist of two activities:

- a request for information on an EU national to the Member State of nationality, or

⁵⁷⁹ See the Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, *OJ L* 93, 7.4.2009, pp. 33-48.

⁵⁸⁰ See the Report from the Commission to the European Parliament and the Council concerning the exchange through the European Criminal Records Information System (ECRIS) of information extracted from criminal records between the Member States, COM(2017) 0341 final, Brussels, 29.6.2017.

⁵⁸¹ See the Council Framework Decision 2008/675/JHA on taking account of convictions in the Member States of European Union in the course of new criminal proceedings, *OJ L* 220, 15.8.2008, p. 32.

⁵⁸² Offences and penalties have been coded in order to facilitate the exchange of information – see Article 4 of the ECRIS Regulation, and the Annexes A and B attached to the legislative text.

⁵⁸³ According to Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, *OJ L* 93, 7.4.2009, pp. 23-32.

- a notification from one Member State to the one of nationality on a new conviction, or on an update of the information previously shared.

In its latest report, the European Commission highlighted that in 2019 the number of requests for information and the related answers was three times higher than the number of notifications, yet '[t]his dramatic increase in the requests for information is due mostly to the shift in the use of the ECRIS, which is not anymore mainly used for the purpose of criminal proceedings, but also more and more for purposes other than criminal proceedings'⁵⁸⁴. Concretely, the statement claims that the ECRIS is consulted in the following circumstances: by individuals, in order to access their own criminal records; by recruiters for professional or organised voluntary activities; by administrators for their activities, and by individuals to obtain a permit to carry a weapon or obtain a different nationality. In addition, the report points out that the ECRIS allows the exchange of information on third country nationals, though this constitutes a minimal part of the overall information exchange.

The new Proposal for a centralised system dedicated to convicted third country nationals was announced in February 2017 as Directive amending the ECRIS Decision⁵⁸⁵. The Directive would have imposed on Member States the duty to store convicted aliens' fingerprints to 'securely and efficiently identify convicted third country nationals' because of the widespread use of unreliable identity documents and the numerous aliases used by criminals⁵⁸⁶. The first initiative proposed the compulsory fingerprinting of all categories of crimes and of all convictions, which raised proportionality concerns among the Member States that would rather limit the collection of this data to one of the following conditions: serious crimes⁵⁸⁷, to the degree allowed by the Member States' national laws, to a pre-established common threshold, or to a list of offences. At that time, the possibility of establishing a unique, centralised system

⁵⁸⁴ See the Report from the Commission to the European Parliament and the Council concerning the exchange through the European Criminal Records Information System (ECRIS) of information extracted from criminal records between the Member States COM(2020) 778 final, Brussels, 29.6.2017. A chronological overview on the history of Member States' connection to ECRIS is available in the Commission Staff Working Document, Accompanying the document Report from the Commission to the European Parliament and the Council concerning the exchange through the European Criminal Records Information System (ECRIS) of information extracted from criminal records between the Member States, SWD(2020) 378 final, Brussels, 21.12.2020, para. 2.8. In this report, the European Commission underlined that many Member States did not send notifications on new convictions nor the relevant updates, but it also admit that some interconnections (9.8%) were missing. Spain was found to be the sole Member State in exchanging information with the other twenty-seven Member States.

⁵⁸⁵ See the Council of the EU, *ECRIS/TCN: Proposal for a Directive amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS) and replacing Council Decision 2009/316/JHA - next steps - debate on crime categories for which fingerprints can be exchanged*, 6691/17, Brussels, 24 February 2017.

⁵⁸⁶ *Ibidem*.

⁵⁸⁷ Member States concretely referred to "serious crimes" as defined in the European Arrest Warrant Framework Decision, and Article 2(2) of the Europol Regulation.

storing identity information of convicted persons, as well as their complete conviction information, was also addressed. Yet, no political support was given by the delegations⁵⁸⁸. Judicial cooperation in the criminal field is indeed a sensible policy that Member States still jealously guard under the wing of sovereignty which limits EU intervention to the minimum required. Therefore, in this area, Member States claimed that new legislative measures shall be kept technologically neutral⁵⁸⁹.

In June 2017, the ECRIS-TCN Regulation was proposed as an autonomous legislative solution on the basis of Article 82(1)(d) TFEU⁵⁹⁰. The European Commission maintained that the ECRIS was not effectively used for third country nationals because of the administrative burden that the lack of an EU nationality would cause. Indeed, in order to find whether a migrant subjected to a final decision⁵⁹¹ had been previously convicted in another Member State, the requesting authority should have sent bilateral demands to all the other Member States. Therefore, the ECRIS-TCN project was revised as a centralised system and it was presented as a supportive measure for cooperation between judicial authorities in the criminal field⁵⁹². However, from the very beginning of the negotiations it was agreed that the central system should have not stored conviction data because ‘[m]ost Member States want to maintain full control over their conviction data, as well as over the decision whether or not to provide that data in response to an individual request’⁵⁹³. The ECRIS-TCN should have merely allowed the central authority to individualise the Member State/s hosting conviction information on a third country national by inserting the individual’s data on the basis of a hit/no-hit mechanism. In

⁵⁸⁸ ‘It was observed that technological neutrality of the system is important’ in Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European criminal records information system (ECRIS-TCN system) and amending Regulation (EU) No. 1077/2011 - Summary of the proceedings of the COPEN meeting on 18 July 2017*, 11445/17, Brussels, 31 August 2017, p. 2.

⁵⁸⁹ *Ibidem*.

⁵⁹⁰ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011*, 10940/17, Brussels, 3 July 2017.

⁵⁹¹ *Ibid.*, p. 11.

⁵⁹² See the Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, PE/88/2018/REV/1, OJ L 135, 22.5.2019, pp. 1-26 (hereinafter the ECRIS-TCN Regulation).

⁵⁹³ See the Commission Staff Working Document, Analytical Supporting Document Accompanying the document Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless people (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011, SWD(2017) 248 final, Brussels, 29.6.2017, p. 6.

this sense, Member States were asked to store the identity information of convicted third country nationals, including biometrics – fingerprints and facial images in the system⁵⁹⁴ and, where available, in the national database⁵⁹⁵ – according to the retention period applicable to their national system. All in all, criminal convictions and offences are one of the categories of personal data benefitting from a special regime under the label of “sensitive data”⁵⁹⁶. Article 10 of the GDPR provides that when this data is treated by public authorities that are not covered by the LED⁵⁹⁷ or private parties⁵⁹⁸, then:

‘Processing [...] shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects [...] Any comprehensive register of criminal convictions shall be kept only under the control of official authority’.

This data shall be kept along with records of processing activities, the carrying out of data protection impact assessments and the designating of a data protection officer.

When launched, the hit/no-hit search will then match the data with additional identity data stored in the system and, takes the following steps: it compares biometrics with a one-to-many search thanks to the AFIS, and then matches the alphanumeric information with the additional data stored in the Central System. In this respect, the ECRIS-TCN Regulation specifies that, for the time being, facial images should only be used to confirm the identity of the third country

⁵⁹⁴ See the Article 6 of the ECRIS-TCN Regulation that addresses the use of facial images. For the moment, facial images included in the ECRIS-TCN system may only be used for the purpose of verification of identification. In the future, it is not excluded that, following the development of the facial recognition software, the facial images might be used for automated biometric matching, provided that the technical requirements to do so have been met.

⁵⁹⁵ In order to ensure the maximum effectiveness of the system, this Article also obliges the Member States to create records in the ECRIS-TCN system of historical convictions of third country nationals – i.e., convictions handed down prior to the entry into force of the ECRIS-TCN Regulation. Under Article 25, it is specified that Member States should complete this process within twenty-four months after the entry into force of the ECRIS-TCN Regulation. Before the difficulties that some Member States may have faced with regard to the insertion of biometrics of previous convictions, the Council found an agreement to delimit the scope of the Article to: the data must already be collected and stored in the national databases – i.e., no new data must be collected; fingerprints can only be inserted when they meet the quality criteria, as will be set out in the implementing act to be adopted according to Article 10(1)(b); the data for convictions handed down prior to the date of entry into force of the ECRIS-TCN Regulation, should be entered into the system within 2 years after the entry into force of the Regulation (Article 38 (2)), and fingerprints can only be entered in case the respective conviction data is valid in criminal records – i.e., only during the retention period of the conviction. Confront the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European criminal records information system (ECRIS-TCN system) and amending Regulation (EU) No. 1077/2011 - Thematic discussion paper*, 12574/17, Brussels, 4 October 2017, p. 6.

⁵⁹⁶ Criminal convictions are data relating to actual criminal convictions pronounced by a court or similar public authority while criminal offences include data out of an actual conviction. The latter may be extended so as to include also “suspicious” according to Ludmila Georgieva, “Article 10. Processing of personal data relating to criminal convictions and offences”, in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *op. cit.*, pp. 385-390, p. 389. Security measures includes criminal offences that stop short of a criminal conviction.

⁵⁹⁷ For the purposes under Articles 2(2)(d) and 1(1) LED by the authorities listed under Article 3(7).

⁵⁹⁸ See recital (19) of the ECRIS-TCN Regulation only when established by national law.

national (meaning, for biometric verification purposes) and, when the technical and political requirements are met, facial images will also be used for automated biometric matching (in other words, in the frame of a biometric identification)⁵⁹⁹. In the case of a hit, the requesting central authority will be informed as to which Member State is hosting the criminal records, the reference data, and any associated identity data related to the individual⁶⁰⁰. The identification of the individual enables the Member State to send an *ad hoc* request for information to the Member State that is seeking to convict the individual⁶⁰¹. This request is sent through the ECRIS communication channel via the national Central Authority⁶⁰².

The choice of a centralised system instead of a decentralised communication channel was criticised by the EDPS as it did not follow the cost-effectiveness approach maintained by the European Commission⁶⁰³. Although both the EDPS and the FRA opted for a decentralised solution, the European Commission insisted that a centralised system would be more compatible with the data security and data minimisation principles as it would avoid the bilateral exchange of information between Member States, without first knowing if the Member State from which the information was requested actually held the relevant information⁶⁰⁴. According to the EDPS the inefficiencies within the ECRIS did not sufficiently justify the establishment of a large-scale IT system in light of the principles of necessity and proportionality⁶⁰⁵. The fact that EU and third country nationals would be treated differently, where only the latter would have their data centrally stored in a system, also raises concerns with regard to the prohibition of no discrimination⁶⁰⁶. This situation was aggravated because of the differences in treatment between EU citizens and third country nationals when dual

⁵⁹⁹ See recital (24) of the ECRIS-TCN Regulation.

⁶⁰⁰ See Article 7 of the ECRIS-TCN Regulation.

⁶⁰¹ The proceeding is described in the Commission Staff Working Document, SWD(2017) 248 final, Brussels, 29.6.2017, p. 4.

⁶⁰² See the Directive (EU) 2019/884 of the European Parliament and of the Council of 17 April 2019 amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, PE/87/2018/REV/1, OJ L 151, 7.6.2019, pp. 143-150.

⁶⁰³ Indeed, the European Commission advocated to a centralised system as the preferred solution in terms of costs efficient, technical complexity and maintenance as the implementation of a centralised database would have saved seventy-eight millions of euros than the existing ECRIS solution.

⁶⁰⁴ See the Commission Staff Working Document, SWD(2017) 248 final, Brussels, 29.6.2017, pp. 11 and 12.

⁶⁰⁵ Moreover, the Opinion of the EDPS No. 11/2017 on *the Proposal for a Regulation on ECRIS-TCN*, Brussels, 12.12.2017, denounced that the proposal should have been accompanied by an impact assessment to balance its impact on fundamental rights since the European Commission was relying on the evaluation made on the Proposal ECRIS Directive which was not accepted by the EDPS.

⁶⁰⁶ As for discrimination, the European Commission was of the opinion that: '[...] the different treatment does not lead to any substantial disadvantages for [third country nationals] and the objectives of the initiative could not be achieved equally well in a decentralised manner [...] Although there are some differences between the centralised and decentralised options, these differences are not so important that they would justify spending significantly more on the creation of a decentralised solution'.

nationals with at least one nationality from one of the Member States were concerned. The insertion of this category of person in the ECRIS-TCN was justified ‘since these people can otherwise "hide" one of their nationalities’⁶⁰⁷, but its provision found strong opposition in the European Parliament, that aimed to treat all the EU citizens equally, notwithstanding their dual nationality⁶⁰⁸. The need to insert this category of individuals in the ECRIS-TCN should have been further justified. As the EDPS maintained, under the ECRIS regulation, Member States were not obliged to store the fingerprints of EU citizens⁶⁰⁹ and the hit generated by the launching of the identification procedure should have already been perceived as an intrusion on the individual’s right to the protection of personal data⁶¹⁰. On the contrary, the storage of dual nationals’ identity data was supported by the delegations that proposed the creation of a unique, centralised database for the criminal records of EU citizens⁶¹¹. The text resulting from the ECRIS-TCN Regulation attempts to equalise the conditions of storage of the dual nationals’ personal data with the conditions set forth in the ECRIS. As a result, it establishes that the fingerprints of dual nationals shall be collected according to national law in light of a criminal proceeding, or for other purposes⁶¹². The Regulation also provides that dual nationals can have their data stored in the ECRIS-TCN if the competent authority knows that the person has a

⁶⁰⁷ See Article 2 of the ECRIS-TCN Regulation and the Council of the EU, 11445/17, Brussels, 31 August 2017, p. 6, and the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European criminal records information system (ECRIS-TCN system) and amending Regulation (EU) No. 1077/2011 - Revised text following COPEN meeting on 11 and 12 September 2017*, 12187/17, Brussels, 19 September 2017, p. 11.

⁶⁰⁸ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU No 1077/2011) - Revised four column table*, 7521/18, Brussels, 12 April 2012.

⁶⁰⁹ See the Opinion of the EDPS No. 11/2017 on the *Proposal for a Regulation on ECRIS-TCN*, Brussels, 12.12.2017, para. 22.

⁶¹⁰ Since it reveals that the person has been subject to criminal convictions, though the criminal conviction is not contained therein – *ibid.*, para. 30. The European Parliament amendment No. 14 suggested that ‘[a] hit in the ECRIS-TCN system by itself should not therefore be used to undermine the principle of equality before the law, the right to a fair trial, the presumption of innocence or the general prohibition of discrimination’, but this was not incorporated in the text – see the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU No 1077/2011) - Four column table with Presidency suggestions/comments*, 5505/18, Brussels, 9 February 2018, p. 18.

⁶¹¹ The so called ECRIS4ALL that was presented in the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011 - Presidency note with questions*, 10828/18, Brussels, 10 July 2018.

⁶¹² See recital (9) of the ECRIS-TCN Regulation *in fine*.

foreign nationality⁶¹³, though these restrictions were not inserted in the body of the act, as suggested by the European Parliament, but in the recitals⁶¹⁴.

Another point of discussion in the preparatory works concerned the categories of criminal offences – including less serious crimes – for which Member States would have been obliged to enter the individuals’ fingerprints – and the fact that the fingerprints may have been collected for reasons other than criminal proceedings under national law⁶¹⁵. This would have required a common understanding on “criminal offences” that so far has not been agreed upon in any EU instrument⁶¹⁶. The Council proposed to define the obligation on the basis of the sanction imposed on a third country national, such as a custodial sentence in relation an intentionally committed criminal offence⁶¹⁷. With respect to the rigid original obligation proposed by the European Commission, the Member States’ obligation in using the ECRIS-TCN were lessened during the negotiations so that Member States may choose to insert fingerprints of third-country nationals who have received a custodial sentence of at least six months, or third-country nationals who have been convicted of a criminal offence which is punishable under the law of the Member State concerned by a custodial sentence of a maximum period of at least twelve months⁶¹⁸. Moreover, the ECRIS-TCN may not be used by the States when it is considered inappropriate given the type of crime – e.g., in certain types of urgent criminal proceedings, in cases of transit, when criminal record information was obtained recently via the ECRIS system – or in respect of minor offences – in particular minor traffic offences, minor offences in relation to general municipal regulations, and minor public order offences⁶¹⁹. In practice, the ECRIS-TCN can be consulted to check whether any Member State holds criminal records when the

⁶¹³ See recital (22) of the ECRIS-TCN Regulation.

⁶¹⁴ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011* - Presidency note, 11310/18, Brussels, 6 September 2018.

⁶¹⁵ See Article 5(5) of the ECRIS-TCN Regulation.

⁶¹⁶ On this topic, see Stefania Carnevale, Serena Forlati, and Orsetta Giolo, *loc. cit.*

⁶¹⁷ Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European criminal records information system (ECRIS-TCN system) and amending Regulation (EU) No. 1077/2011* [First reading] - Policy debate, 12596/17, Brussels, 2 October 2017, pp. 3-5.

⁶¹⁸ Article 5(1)(b) of the ECRIS-TCN Regulation. The European Commission reacted to this decision by complaining the fact that the system would be less efficient without storing biometrics in all cases, Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European criminal records information system (ECRIS-TCN system) and amending Regulation (EU) No. 1077/2011* - Confirmation of the final compromise text with a view to agreement, 15701/18, Brussels, 18 December 2018.

⁶¹⁹ See recital (20) of the ECRIS-TCN Regulation.

authority is not aware of the individual's citizenship. For their part, facial images are inserted in the central system only if the collection and storage of this type of biometrics is required under national law⁶²⁰. It should be remembered that the EDPS' position on biometrics is that this is sensitive data whose usage shall be limited to the absolute minimum required – i.e., when the individual's identity cannot be ascertained by other means.

A third important point to be noted pivoted around the exercise of individuals' data protection rights and the Member State's responsibility to correct or delete the data of convicted persons. Member States clearly affirmed that they sought to maintain their control of their data and would not have permitted any interference by other Member States. As a consequence, and although the data subject was granted the right to submit a request of access, erasure, and restriction of processing to any central authority, the request would be executed only by the convicting Member State⁶²¹. Along the same lines, any attempt to seek a remedy shall be brought against the sole Member State. The possibility advanced by the European Parliament that the data subject should have been issued a certificate to testify that the ECRIS-TCN was searched, also in case where no record was found, was not accepted.

Last but not least, the Proposal clarified that, apart from the support that the ECRIS-TCN would bring to criminal judicial authorities, previous convictions would be taken into account regarding decisions on ending a legal stay, a return, and the refusal of entry concerning third country nationals posing a threat to public policy, public security or national security⁶²². These circumstances are firstly translated into the SIS II alerts on refusal of entry or the decision to end an individual's stay so that competent authorities issuing this type of alert can take into account previous convictions. From a border management perspective, being a threat to public policy, internal security, public health or the international relations of any of the Member States is grounds for refusing entry to third country nationals according to the Schengen Borders Code⁶²³, and in those cases where a SIS II alert has not been issued (yet) the ECRIS-TCN is useful. Hence, the possibility to access the ECRIS-TCN drew attention to the ability of other systems directly implicated in the management of external borders such as the ETIAS⁶²⁴ and

⁶²⁰ See Article 5(3) of the ECRIS-TCN Regulation.

⁶²¹ See Article 25 of the ECRIS-TCN Regulation and, especially, the position of Germany in the Council of the EU, 12187/17, Brussels, 19 September 2017, pp. 35 and 36.

⁶²² The possibility to use ECRIS-TCN for immigration law decisions has been well highlighted by Evelien Brouwer, "Large-Scale Databases and Interoperability in Migration and Border Policies: The Non-Discriminatory Approach of Data Protection", *European Public Law*, Vol. 26, No. 1, 2020, pp. 71-92, p. 84, who quickly but significantly retraces the development of large-scale IT systems in the last twenty years.

⁶²³ Article 6 of the Schengen Borders Code.

⁶²⁴ See the discussions on Council of the EU, 12574/17, Brussels, 4 October 2017, pp. 2-4. Article 20 of the ETIAS Regulation excluded the automated check to the ECRIS-TCN since the European Parliament was clearly against this possibility.

the VIS to identify individuals. Article 1 of Regulation (EU) 2021/1151 expands the scope of the ECRIS-TCN to include border management in accordance with the ETIAS Regulation. In this sense:

‘The result of a search in the Central System may only be used for the purpose of making a request according to Article 6 of Framework Decision 2009/315/JHA, a request referred to in Article 16(4) of this Regulation, or for the purposes of border management [and facilitating and assisting in the correct identification of persons registered in the ECRIS-TCN system]’.

In the case of a hit, a flag in the ETIAS indicates if there is a match with the ECRIS-TCN, if the person was convicted in a Member State. However, the European Parliament was the major obstacle in impeding the insertion of the automated check to the ECRIS-TCN in the ETIAS Regulation, and imposed a monitoring requirement for the hits resulting when the ETIAS queried the ECRIS-TCN. The EDPS was opposed to the enlargement of the ECRIS-TCN’s purposes⁶²⁵ and firmly criticised the possibility of requesting information beyond the scope of a criminal proceeding⁶²⁶:

‘[i]t should not be easily accepted that since the data is already stored in an IT system, it could just as well be regularly used for other purposes than those for which it was initially collected, without explicit justification or transparent debate, and with potentially a bigger impact on life of individuals. [T]he processing of data, even if regarded as proportionate for a specific purpose, may become inadequate or excessive when the same data further processed for additional purpose’⁶²⁷.

However, at least one of the other purposes for which the ECRIS-TCN can be consulted can be positively evaluated: the consultation by recruiters in areas involving children that was inserted by the European Parliament⁶²⁸ as this enhanced access may help to protect minors.

⁶²⁵ Opinion of the EDPS No. 11/2017 on *the Proposal for a Regulation on ECRIS-TCN*, Brussels, 12.12.2017, para. 21. Concretely for the ETIAS see the Council of the EU, 7553/19, Brussels, 15 March 2019, p. 5. The EDPS noted that not only the data stored in the ECRIS-TCN would have been processed for a ‘far beyond purpose’ than the one initially envisaged, but also that the ETIAS Central Unit and the ETIAS National Unit would have access for verification and manual processing respectively – see Articles 22 and 26 of the ETIAS Regulation. Thus, the ETIAS Central Unit would have access to the data flagged in the ECRIS-TCN that will evidence that the conviction refers to a terrorism or serious criminal offence.

⁶²⁶ See the Opinion of the EDPS No. 11/2017 on *the Proposal for a Regulation on ECRIS-TCN*, Brussels, 12.12.2017, para. 26, on Article 7 of the ECRIS-TCN Regulation whose scope has been finally restricted thanks to the European Parliament to: checking a person’s own criminal record at his or her request; security clearance; obtaining a licence or permit; employment vetting; vetting for voluntary activities involving direct and regular contacts with children or vulnerable persons; visa, acquisition of citizenship and migration procedures, including asylum procedures, and checks in relation with public contracts and public examinations.

⁶²⁷ See the Council of the EU, 7553/19, Brussels, 15 March 2019, p. 4. The EDPS recalled the obligation to realise an impact assessment according to Article 39 of the DPRED for data processing of high risk to the rights and freedoms of data subjects and that the exception of paragraph (9) ask to: first, the existence of a legal basis regulating the processing operation or set of processing operations and, second, the realisation of an impact assessment for the proposed legal basis.

⁶²⁸ See recital (2) in the document Council of the EU, 5505/18, Brussels, 9 February 2018.

From the ECRIS-TCN Proposal, it is clear that the ECRIS-TCN is a system that has been designed with interoperability in mind⁶²⁹. In this sense, the management of the system has been handed to eu-LISA⁶³⁰ whose mandate is split between both the eu-LISA Regulation and the ECRIS-TCN Regulation. Additionally, the ECRIS-TCN Regulation allows that, after three years of implementation, the European Commission may decide to propose an enlargement of the system so as to include additional data⁶³¹. Indeed, with the adoption of the ETIAS consequential amendments, the ECRIS-TCN Regulation has been revised so as to officially join the interoperability architecture⁶³². This confirms that the last generation of large-scale IT systems – namely the EES, the ETIAS and the ECRIS-TCN – constitutes the basis of the interoperability infrastructure, while the old one – i.e., the SIS, the Eurodac, and the VIS – will be progressively adapted to the interoperability design so as to eventually join the other components, as we will explore in the following Chapters.

⁶²⁹ In the Proposal it is clearly stated that the ECRIS-TCN will have: a ESP to query the system; a sBMS to match biometric templates, and a CIR with alphanumeric data to detect multiple identities in different databases. This infrastructure would also facilitate the implementation of bilateral interconnect between ECRIS-TCN and the other systems.

⁶³⁰ see the Commission Staff Working Document, SWD(2017) 248 final, Brussels, 29.6.2017, p. 10: ‘In evaluating the complexity, the main consideration was that the implementation of a central ECRIS TCN system could benefit from the experience of eu-LISA with proven technologies and successful implementation of already existing fully automated centralised systems such as EURODAC and the VIS’.

⁶³¹ See the Council of the EU, 5505/18, Brussels, 9 February 2018, p. 11.

⁶³² See Article 2(4)(b) of Regulation (EU) 2021/1151.

CHAPTER IV

THE INSTITUTIONALISATION OF THE EUROPEAN UNION'S COMPETENCE ON THE OPERATIONAL MANAGEMENT OF LARGE-SCALE IT SYSTEMS

Multi-purpose IT systems¹ are the result of an entire comprehensive policy-oriented implementation of Union competences within the AFSJ that legitimised the provision of new access rights to national authorities and Union agencies². In the last twenty years, large-scale IT systems have fallen into a legislative loop aimed at increasing their use under the aegis of the most extensive technological revolution ever. However, the stretching of large-scale IT systems' "ancillary purposes" is preventing the systematisation of the legislative measures regulating the systems as the co-legislators jump from one legal basis to the other when justifying their expansion.

The adoption of new instruments touching upon different legal bases regarding the freedom, security and justice fields led to the foundation of eu-LISA³. eu-LISA represents a fair compromise in the implementation of EU shared policies where both Member States' authorities and Union staff cooperate without (supposedly) pre-empting the Member States' implementing powers. Challenging the limits established by the principle of conferral, eu-LISA's mandate ensures the simultaneous implementation of almost all the freedom, security and justice policies by operationally managing large-scale IT systems. Under eu-LISA, the European Commission and the Member States cooperate in the implementation of existing and future large-scale IT systems.

The transfer of personal data to third countries not subjected to the EU *acquis* and to international organisations operated by a Union agency is regulated by the EUDPR. Interestingly, the regime foreseen in the latter is more fragmentated than the ones established by the GDPR and the LED. According to Articles 46(2)(a) and 46(3)(b) of the GDPR, personal data can be transferred through administrative instruments and, specifically:

- a legally binding and enforceable instrument, or

¹ Niovi Vavoula, 2020, *op. cit.*, p. 133.

² Evelien Brouwer, "A Point of No Return in Purpose Limitation? Interoperability and the Blurring of Migration and Crime", *Blog Forum: Interoperable Information Systems in the EU Area of Freedom, Security and Justice*, no date is specified, available at www.migrationpolicycentre.eu.

³ Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011, PE/29/2018/REV/1, OJ L 295, 21.11.2018, pp. 99-137 (eu-LISA 2018 Regulation hereinafter).

- an arrangement that includes ‘enforceable and effective data subject rights’ as authorised by the competent supervisory authority.

According to Article 37(1)(a) and (b) of the LED, personal data can be transferred through a ‘legally binding instrument’ or the controller’s own assessment of which competent supervisory authority must be informed. Therefore, the possibility of concluding soft law arrangements for transmitting personal data for PJCCM purposes is excluded. Notably, the EUDPR follows the GDPR-LED dichotomy, but it also moves away from their regimes since: it makes safe Union agencies’ cooperation agreements – i.e., Article 94(1)(c) EUDPR – as well as each PJCCM agency’s mandate – i.e., Article 94(2) EUDPR – to maintain or introduce more specific provisions. We believe that these changes should be justified in the light of the operational activity deployed by each Union agency to achieve their missions, though it is not clear whether the limits set down by the delegation doctrine are always respected.

The following section analyses the institutionalisation of the EU operational competences on the management of large-scale IT systems under eu-LISA. First, the delegation doctrine developed by the CJEU, as its judgment in *Meroni* is briefly presented⁴ to highlight how executive operational competences from the European Commission (or the Council) are delegated to Union agencies. Notwithstanding the types of tasks Union agencies execute, the practice of delegation must be realised in full respect of the principles enshrined in the founding Treaties and, first of all, the allocation of competences between the EU institutions must be respected – i.e., the principle of institutional balance. Afterwards, we will turn toward the foundation of eu-LISA and the upgrading of its mandate to clarify its role *vis-à-vis* the processing of data stored in the systems and, consequently with Article 16 TFEU. At this stage of our research, it would not come as a surprise if Article 16(2) TFEU was not underpinning eu-LISA’s mandate, though it would be appropriate if we discover that ‘[...] the protection of personal data is one of the essential aims or components of the rules adopted by the EU legislature, including those falling within the scope of the adoption of measures covered by the provisions of the FEU Treaty relating to judicial cooperation in criminal matters and police cooperation [...]’⁵. Once the range of eu-LISA’s mandate is clarified, we could assess whether the agency contributes to the external reach of the interoperability framework set down by Regulations (EU) 2019/817 and 2019/818, i.e., whether eu-LISA has access to the data stored

⁴ Herwig C.H. Hofmann, Gerard C. Rowe, and Alexander H. Türk, *op. cit.*, p. 223: ‘Delegation is a general phenomenon in implementation of EU policies with a wide variety of actors in the European administrative space, such as European agencies, networks, and private actors’.

⁵ *Opinion 1/15*, para. 39.

therein and if it is entitled to conclude administrative agreements or arrangements that enable its transfer.

1. Basic principles underpinning the delegation doctrine

EU agencies⁶ are created to efficiently implement the European Commission's functions regarding the correct implementation of EU law, or to enhance the European Commission's executive capacity in respect of the principle of indirect execution administration⁷. For this reason, they constitute a fair compromise between supranationalism and intergovernmentalism: Member States accept their presence in order to implement common policies agreed at the legislative layer⁸, and the European Commission sees this arrangement as the only way to reach a significant degree of integration⁹. In reality, Union agencies are not functionally independent from the political power – as they respond to the needs of decentralisation¹⁰ –, but a certain degree of autonomy from an administrative and financial perspective allows them to accomplish their specific objectives¹¹.

Despite the agencification phenomenon being well established¹², scholars have mainly focused on the delegation of normative competences, that is, their empowerment to adopt binding or soft law decisions. However, literature on agencies makes abundant references to

⁶ Merijn Chamon, *EU Agencies: Legal and Political Limits to the Transformation of the EU Administration*, Oxford, Oxford Studies in European Law, 2016, p. 10, defines EU regulatory agencies as '[...] permanent bodies under EU public law established by institutions through secondary legislation, and endowed with their own legal personality'. The permanence requisite, precisely, is what Prof. Chamon identifies to distinguish EU regulatory agencies from the executive ones, with the sole exception of the European Agency for Reconstruction and the European Network and Information Security Agency that, although being regulatory agencies, they had been established for a predefined period of time.

⁷ See Cecilia Corsi, *Agenzia e agenzie: una nuova categoria amministrativa?*, Torino, Giappichelli Editore, 2005, pp. 38-41; Ellen Vos, "Reforming the European Commission: what role to play for EU agencies?", *Common Market Law Review*, No. 37, 2000, pp. 1113-1134, and Michelle Everson, "European Agencies: Barely Legal?", in Michelle Everson, Cosimo Monda, and Ellen Vos, *European Agencies in between Institutions and Member States*, The Netherlands, Kluwer Law International BV, 2014, pp. 49-70, at p. 56, highlighting that after the bovine spongiform encephalopathy crisis the need of transparency and permanency made the European Commission opting for regulatory agencies instead of committees.

⁸ Merijn Chamon, Herwig C.H. Hofmann, and Ellen Vos, *The External Dimension of EU Agencies and Bodies: Law and Policy*, Cheltenham, Edward Elgar Publishing, 2019, p. 2.

⁹ Which makes Merijn Chamon, 2016, *op. cit.*, p. 50, placing them between "indirect" and "direct" forms of administration while giving birth to "shared administration" forms. Ellen Vos, "European Agencies and the Composite Executor", in Michelle Everson, Cosimo Monda, and Ellen Vos, *op. cit.*, pp. 11-47, p. 15: 'The creation of agencies herewith responded to the need for more uniformity in the implementation of EU policies where the harmonization model appeared to be less attractive while upholding the EU's system of decentralized implementation'.

¹⁰ Edoardo Chiti, *Le agenzie europee*, Padova, CEDAM, p. 462.

¹¹ Marta Simoncini, *Administrative Regulation Beyond the Non-Delegation Doctrine: A study on EU Agencies*, Oxford, Hart Publishing, 2018, and Cecilia Corsi, *Agenzia e agenzie: una nuova categoria amministrativa?*, Torino, Giappichelli Editore, 2005, pp. 38-41.

¹² Renaud Dehousse, "Misfits: EU Law and the Transformation of European Governance", in Christian Joerges and Renaud Dehousse, *Good Governance in Europe's Integrated Market*, Oxford, Oxford University Press, 2002, pp. 207-216

the execution of ‘operational’ tasks as well, without entering into the analysis of the concept. Operational competence is generally associated with the EU’s power to act more than to legislate¹³. In Prof. Neframi’s words: ‘This is a different kind of competence, which is exercised through measures that are completely at the disposal of the Member States under the principle of indirect administration’¹⁴. As Prof. Neframi underlines, the possibility of the EU to act in the operational layer derogates the Member States’ prerogatives in implementing EU law as it deviates from the principle of indirect administration of Article 197 TFEU¹⁵. Indeed, the execution of EU law is a Member State’s prerogative for which purpose they undertake operational activities, yet when the execution of EU law requires a ‘combined effort’¹⁶ Member States’ cooperation may be more efficient when seeking to achieve goals than relying on fragmented initiatives. From this perspective, EU operational competences represent the last step to be undertaken for the implementation of EU law, that is, its execution “on the territory” and “in direct contact with the people concerned”¹⁷. Recalling Advocate General Van Gerven’s Opinion¹⁸, decision-making consists of three stages:

- first, the exercise of powers at the political level;
- second, the adoption of measures of management and administration, and
- lastly, measures of practical execution.

¹³ Note that the term operational is used in public international law to designate those international organisations that according to José Antonio Pastor Ridruejo, 2021, *op. cit.*, p. 718, are international organisations acting in the ‘international territory, through their own means, or through those means Member States make available to them, but deciding their usage themselves’. In this sense, the term “operational” recalls the French model of administration that tends to distribute individualised missions according to Gérard Marcou, “Le thème de l’agence et la réforme des administrations centrales”, in Joël Molinier, *Les agences de l’Union européenne*, Brussels, Bruylant, 2011, pp. 3-36, p. 8, who highlights that the EU agency model is in constant tension between the French and the US ones which results in a debate on the limits chargeable to EU agencies’ empowerment.

¹⁴ See Eleftheria Neframi, “La répartition des compétences entre l’Union Européenne et ses États Membres en matière d’immigration irrégulière”, in Dubin Laurence, *La légalité de la lutte contre l’immigration irrégulière par l’Union européenne*, Brussels, Bruylant, 2012, pp. 35-63, p. 46 (our own translation). The author underlines that the principle of indirect administration of EU Law bound the Member States to adopt the relevant national legislation and to act accordingly in the light of the principle of loyal cooperation.

¹⁵ See Article 291(1) of the TFEU: ‘Member States shall adopt all measures of national law necessary to implement legally binding Union acts’. Herwig C.H. Hofmann, “General Principles of EU law and EU administrative law”, in Catherine Barnard and Steve Peers, *op. cit.*, pp. 212-242, highlights that: ‘Administrative law is part of public law enabling and constraining administrative conduct, that is, activity designed to implement EU law. The essence of EU administrative law are therefore rules and principles governing the procedures for exercising administrative functions and the organisation of the institutions and bodies exercising these functions’. Also, Herwig C.H. Hofmann, Gerard C. Rowe, and Alexander H. Türk, *op. cit.*, p. 99: ‘The Member States therefore generally enjoy the right to determine their internal organization, and their procedural provisions in the area of implementation of EU law’.

¹⁶ Merijn Chamon, 2016, *op. cit.*, p. 41.

¹⁷ Florian Aumond, “Responsabilité des organisations internationales et droits fondamentaux. L’exemple de l’ONU dans le contexte de l’administration et de la gestion des camps de réfugiés et de déplacés internes par le HCR”, *Les responsabilités*, 2018, pp. 5-24, p. 6.

¹⁸ Opinion of Advocate General Van Gerven, C-137/92 P, *Commission of the European Communities v BASF AG, Limburgse Vinyl Maatschappij NV, DSM NV, DSM Kunststoffen BV, Hüls AG, Elf Atochem SA, Société Artésienne de Vinyle SA, Wacker Chemie GmbH, Enichem SpA, Hoechst AG, Imperial Chemical Industries plc, Shell International Chemical Company Ltd and Montedison SpA*, 29 June 2003, EU:C:1994:247, para. 41.

Only the latter would integrate the concept of EU operational competences as it is directed at regulating the practical work of public authorities, but as with the second type of measures, this may be delegated to EU agencies according to the revised *Meroni* doctrine analysed *infra*¹⁹. Arguably, the founding Treaties do not expressly state when the Union is conferred operational competences, and it may be difficult to delimit the constitutional boundaries in light of the horizontal subdivision of competences set forth in the founding Treaties²⁰. Yet, some “practical” legal bases, especially within the AFSJ²¹, can be pointed out. For instance, Article 67 of the 1997 TEC empowered the Council to adopt ‘measures to ensure cooperation between the relevant departments of the administrations of the Member States in the areas covered by [Title IV TFEU]²², as well as between those departments and the European Commission’²³, and was firstly used for establishment of the ARGO program²⁴, the Immigration Liaison Officers network²⁵, and the EBCG Agency²⁶. Today, Article 74 TFEU covers a strategic position that supersedes the entire AFSJ including, and this is a crucial detail, the PJCCM area. Notably,

¹⁹ In the Communication from the Commission to the European Parliament and the Council - European agencies – The way forward, COM(2008) 135 final, Brussels, 11.3.2008, the European Commission inserted within the so-called “regulatory agencies” the agencies in charge of operational activities and it made reference to the following ones: European Agency for Reconstruction; European Agency for Space Programme; Community Fisheries Control Agency; EBCG Agency; Eurojust; Europol and European Union Agencies for Law Enforcement Trainings (CEPOL). Paul Craig, *EU Administrative Law*, Oxford, Oxford University Press, 2018, pp. 151-198, p. 163 ff., proposes another classification for which these agencies would fall within the category of Information and Coordination Agencies whose main tasks are directed at ‘furnishing and analysing the information for the Commission, the Member States, and other related actors’.

²⁰ See Merijn Chamon, Herwig C.H. Hofmann, and Ellen Vos, *The External Dimension of EU Agencies and Bodies: Law and Policy*, Cheltenham, Edward Elgar Publishing, 2019, p. 2.

²¹ On the empowerment of the freedom, security, and justice agencies see Juan Santos Vara, “The EU’s agencies: Ever more important for the governance of the Area of Freedom, Security and Justice”, in Ariadna Ripoll Servent and Florian Trauner, *The Routledge Handbook of Justice and Home Affairs Research*, Taylor and Francis Group, 2017, pp. 445-457, p. 448.

²² Concerning ‘visas, asylum, immigration and other policies related to free movement of persons’.

²³ See the Council of the EU, *Note de Transmission, Document de travail des services de la Commission accompagnant la proposition de règlement du Parlement européen et du Conseil portant création d’un Bureau européen d’appui en matière d’asile – Résumé de l’analyse d’impact*, 6700/09 ADD 2, Brussels, 23 February 2009, p. 4.

²⁴ See the Decision 2002/463/EC adopting an action programme for administrative cooperation in the fields of external borders, visas, asylum and immigration, *OJL* 371, 18.12.2004, pp. 48-49, repealed by Council Decision 2004/867/EC of 13 December 2004 amending Decision 2002/463/EC adopting an action programme for administrative cooperation in the fields of external borders, visas, asylum and immigration, *OJL* 371, 18.12.2004, pp. 48-49. Unfortunately, the list of Programme for administrative cooperation in the fields of external borders, visas, asylum and immigration and of European Refugee Fund projects was not published in the Council of the EU, *Commission Staff Working Document Accompanying document to the Proposal for a Regulation of the European Parliament and of the Council establishing an European Asylum Support Office - Impact assessment*, 6700/09 ADD 1, Brussels, 23 February 2009, p. 86 ff.

²⁵ Council Regulation (EC) No 377/2004 of 19 February 2004 on the creation of an immigration liaison officers network, *OJL* 64, 2.3.2004, pp. 1-4.

²⁶ Jorrit Rijpma, “Hybrid agencification in the Area of Freedom, Security and Justice and its inherent tensions: the case of Frontex”, in Madalina Busuioc, Martijn Groenleer, and Jarle Trondal, *The agency phenomenon in the European Union: Emergence, institutionalisation and everyday decision-making*, Manchester, Manchester University Press, 2012, pp. 84-102, p. 90.

PJCCM is not considered as an EU policy, but as an area of operational cooperation²⁷ that Sicurella describes as a ‘complementary tool’²⁸. This reading explains why the communitarisation of PJCCM competences²⁹ had been challenged by the Member States’ willingness to retain³⁰ coercive powers on national security³¹ by virtue of Articles 72, 73 TFEU and 4(2) TEU³². As Prof. Peers underlines, these limits do not prevent the EU from legislating on the subject³³, but they impede the deployment of a common police force in the Member

²⁷ Henri Labayle, “The institutional framework”, in Valsamis Mitsilegas, Maria Bergstrom, and Theodore Konstadinides, *Research Handbook on EU Criminal Law*, Cheltenham, Edward Elgar Publishing, 2016, 29-48, p. 33.

²⁸ While referring to Article 67(3) TFEU, the author expressly refers to measures of coordination and cooperation between police and judicial authorities and other competent authorities. Rosaria Sicurella, “EU competence in criminal matters”, in Valsamis Mitsilegas, Maria Bergstrom, and Theodore Konstadinides, *op. cit.*, pp. 49-77, p. 54:

‘[...] this provision shows how the significant widening of the scope of European integration (mainly harmonization of national systems), and the combination of the latter with those tools and methods previously developed outside the EC legal order – cooperation among Member States’ authorities. And mutual recognition – supposed to be supported and framed by EU legislation: the integration of EU competence in criminal matters into a single legal order, then, does not only imply the submission not a single European legal regime, but rather the integration into a single legal system of various methods and dynamics (aiming at) guaranteeing their coherence and effectiveness (in the perspective of the achievement of the AFSJ), and combining supra-national characteristics with some inter-governmental ones’.

²⁹ Article 88 TFEU.

³⁰ See Bruno de Witte, “Exclusive Member States Competences – Is there such a thing?”, in Sacha Garben and Inge Govaere, *The division of competences between the EU and the member States*, Oxford, Hart Publishing, 2017, pp. 59-73, p. 60

³¹ According to Nicholas Grief, “EU Law and security”, *European Law Review*, No. 32, 2007, pp. 752-765, p. 755: ‘Public security arguably means the same a national security and also, presumably, “State security”; and each of those terms must be broader than “internal security”. Inevitably the boundaries between “public security” and “public policy” (order public) justifications are not watertight’. On the matter, see also the C-601/15 PPU, *J. N. v Staatssecretaris voor Veiligheid en Justitie*, 15 February 2016, EU:C:2016:84, para. 66:

‘So far as the concept of ‘public security’ is concerned, it is apparent from the Court’s case-law that this concept covers both the internal security of a Member State and its external security and that, consequently, a threat to the functioning of institutions and essential public services and the survival of the population, as well as the risk of a serious disturbance to foreign relations or to peaceful coexistence of nations, or a risk to military interests, may affect public security [...]’.

In C-18/19, *WM v Stadt Frankfurt am Main*, 2 July 2020, EU:C:2020:511, the CJEU rejected the Germany’s pretension of excluding Article 16 of the Return Directive from the scope of EU law in the light of Article 72 TFEU. In the Germany’s point of view, the detention of an irregular migrants pending removal would pose a serious threat to the life and limb of others or to national security and according to its national law this would fall out of the scope of the Return Directive according to its Article 2(2)(b) for which: ‘Member States may decide not to apply this Directive to third-country nationals who: [...] are subject to return as a criminal law sanction or as a consequence of a criminal law sanction, according to national law, or who are the subject of extradition procedures’.

³² Article 4(2) TEU according to which national security remains of the sole responsibility of each Member States, and Article 72 TFEU establishing that Title V cannot affect the exercise of the Member States’ responsibility for the maintenance of law and order and the safeguarding of internal security. This is in line with Article 287 TFEU that excludes the jurisdiction of the CJEU to assess the validity and proportionality of the coercive measures as well as the exercises of the Member States’ responsibility on the maintenance of public order and internal security. Article 73 TFEU, for its part, enables the Member States to ‘[...] organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the competent departments of their administrations responsible for safeguarding national security’.

³³ Coercive measures are usually associated with law enforcement agents, but also the security services – i.e., the intelligent ones – shall be included in the limits of their participation in the law enforcement tasks which are

States' territories³⁴. As a last resort, the added value of Article 74 TFEU's cross-cutting position is the possibility to adopt horizontal legislations enabling the centralisation of the Union's operational competences regarding the whole AFSJ in a single instrument³⁵.

In any case, the founding Treaties³⁶ do not regulate the delegation of neither normative nor operational competences from the institutions to other bodies, except for some specific rules establishing, for instance, Europol³⁷ and Eurojust³⁸ and some indirect references in Articles 15(3), third paragraph, 16(2), and 263 TFEU³⁹. Therefore, these conjectures must be corroborated in light of the CJEU case-law following the historic *Meroni* judgment⁴⁰, that is, the *Romano*⁴¹ and *Short-selling*⁴² judgments.

1.1. The revised *Meroni* jurisprudence

As our research does not aim to present scientific reflections on the delegation doctrine, but takes its cue from it in order to apply it to the chosen research topic, here we recalling the basic

different from the national security ones, according to Steve Peers, *EU Justice and Home Affairs Law, Volume II: EU Criminal Law, Policing, and Civil Law*, Oxford, Oxford EU Law Library, 2016, pp. 28-29.

³⁴ C-715/17, C-718/17 and C-719/17, *European Commission v Republic of Poland*, 2 April 2020, EU:C:2020:257, para. 143 ff., in which Poland and Hungary alleged the no application of the relocation mechanism for security reasons in the light of Article 72 TFEU. The CJEU admitted that even if relocation could have been refused on the basis of 'reasonable grounds', as it is the case when the asylum applicant represents a 'danger to national security or public order' in the territory of the Member State of relocation, a threat to national security or public order shall be assessed on a case-by-case basis. Similarly is C-461/05, *European Commission v Denmark*, December 2009, EU:C:2009:783 para. 51, and of C-38/06, *European Commission v Portugal*, 4 March 2010, EU:C:2010:108, para. 62.

³⁵ See *infra*.

³⁶ Marijn Chamón, Herwig C.H. Hofmann, and Ellen Vos, *op. cit.*, p. 1.

³⁷ Article 88 TFEU.

³⁸ Article 85 TFEU.

³⁹ The latter clarifying that the CJEU is competent to revise the lawfulness of EU agencies' acts which leaves no doubt that ex- second and third pillars agencies are also included – on the contrary, see C-160/03, *Kingdom of Spain v Eurojust*, 15 March 2005, EU:C:2005:168.

⁴⁰ C-9/56, *Meroni & Co., Industrie Metallurgiche, SpA v High Authority of the European Coal and Steel Community*.

⁴¹ C-98/80, *Giuseppe Romano and Institut National d'Assurance Maladie-Invalidité*, 14 May 1981, EU:C:1981:104. The plea concerned an Italian citizen who had benefited: from a Belgian invalidity pension from the 29 August 1970 to the 31 December 1975, from a Belgian retirement pension since 1 January 1976, and from an Italian invalidity pension with retroactive effect going back to 1 September 1970 starting on 1 July 1976. The national plea pivoted around the method of calculation used by the National Institute for Health and Disability Insurance and, specifically, Sr. Romano disputed how the sum that was provisionally paid could exceed the amount of pension arrears due for the period of the pension under the foreign scheme.

⁴² C-270/12, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*, 22 January 2014, EU:C:2014:18. The case concerned the European Securities and Markets Authority established by Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (ESMA), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC, *OJ L* 331, 15.12.2010, pp. 84-119, and empowered by Regulation (EU) No 236/2012 of the European Parliament and of the Council of 14 March 2012 on short selling and certain aspects of credit default swaps Text with EEA relevance, *OJ L* 86, 24.3.2012, pp. 1-24. According to Article 28 of Regulation (EU) No 236/2012, the European Securities and Markets Authority could adopt measures of individual application toward natural or legal persons to safeguard the orderly functioning and integrity of financial markets or to the stability of the whole, or part of, the financial system in the Union.

principles underpinning the CJEU's case law in application of the Union's external relations theory.

- The *nemo pluris iuris* rule, according to which only previously granted powers can be delegated, which lastly recalls the principle of conferral. After *Meroni*, some scholars assumed that the establishment of agencies should not have been conceived as a delegation of powers from the EU institutions to a new body, but rather as a conferral of powers directly attributed by the Member States to the new body. According to this interpretation, *Meroni* would not be applicable to EU agencies provided that their institutionalisation created new powers by virtue of Article 114 TFEU⁴³. Also, the European Commission – and eventually the Council – would be directly empowered by the Member States by virtue of Article 291(1) TFEU⁴⁴. Indeed, Articles 290 and 291 TFEU differ from one another as they speak of the delegation and conferral of powers respectively. However, Prof. Alberti notes that Article 291 TFEU sets forth that the conferral is not decided by the Member States alone, but also by the institutions through an act of secondary law enabling the adoption of instruments of secondary legislation⁴⁵. This interpretation follows what the author defines as the ‘critic approach’, that is, the doctrinal wave developed since the ‘90s with the aim of fostering integration and, consequently, the proliferation of new agencies notwithstanding their constitutional provision. Hence, unlike the principle of conferral that concerns the legislative allocation of competence from the Member States to the EU, delegation regulates the allocation of powers within the delegating authority’s area of competence⁴⁶.

⁴³ The possibility to institutionalise a new agency on the basis of the harmonisation clause has been seen as suspicious by scholars and by the Opinion of Advocate General Jääskinen, C-270/12, *Digital reports (Court Reports - general)*, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*, 12 September 2013, EU:C:2013:562, since it is difficult to relate the agency’s regulatory powers to the harmonisation objectives set forth therein. In this regard, two cumulative conditions have to be satisfied: first, the agency’s mandate shall consist in a measure of approximation laid down by the law, regulation, or administrative action in the Member States; second, the mandate must have as its object the establishment and functioning of the internal market. In *Short Selling*, the CJEU concluded that article 28 of Regulation No 236/2012 fit the scope of Article 114 TFEU, yet its judgment was criticised because of the broad formulation of Article 114 TFEU that would enable the establishment of EU agencies that might only marginally contribute to the harmonisation process.

⁴⁴ This Article preserves the Member States’ prerogative in implementing EU law while leaving the key role to the European Commission ‘[w]here uniform conditions for implementing legally binding Union acts are needed’.

⁴⁵ Jacopo Alberti, *op. cit.*, p. 367 ff.

⁴⁶ On the difference between conferral and delegation see the Opinion of Advocate General Jääskinen, C-270/12, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*, para. 90, noting that the powers delegated to European Securities and Markets Authority under Article 28 of Regulation (EU) No 236/2012 of the European Parliament and of the Council of 14 March 2012 on short selling and certain aspects of credit default swaps Text with EEA relevance, OJ L 86, 24.3.2012, pp. 1-2, came from the EU legislature by virtue of Article 289(3) TFEU, and not from the Member States according to Article 291(4) TFEU.

- The “shift of responsibility” principle requires that the delegated body is liable for its action. Assessing upon whom the burden of responsibility lies means finding whether the delegation of powers actually occurs, or whether the delegated body acts on behalf of the delegating one – i.e., the principal⁴⁷. As Prof. Alberti finds, this implies that the delegating authority must not claim as its own the decisions issued by the delegated authority⁴⁸, but that the latter benefits from a certain degree of autonomy for which its action are controlled by the former and subjected to *ex post* review – which integrates the principle of accountability⁴⁹.
- The principle of express delegation imposes that the delegation of powers not be presumed, but must be explicitly set down for reasons of legality and legal certainty⁵⁰.
- The prohibition on delegating discretionary power is under dispute since the range of non-discretionary power has been interpreted differently by the CJEU. If in *Meroni* the CJEU found that only ‘clearly defined executive power’ could be delegated, in *Romano* it sentenced that ‘acts having the force of law’ could not be delegated, so that binding acts of general application would not be delegable while ‘binding acts in individual cases’⁵¹ would be. However, in *Short Selling* the CJEU ruled that the powers to be delegated must be ‘precisely delineated and amenable to judicial review’⁵². Specifically, the CJEU noted that in light of Articles 263 and 277

⁴⁷ According to Andrea Ott, Ellen Vos, and Florin Coman-Kund, “European Agencies on the Global Scene: EU an International Law Perspectives”, in Michelle Everson, Cosimo Monda, and Ellen Vos, *op. cit.*, pp. 87-122, p. 101:

‘In the *Meroni* cases, the Court indeed distinguished between a ‘true’ delegation of the powers conferred upon the delegating authority and a situation where the authority grants the powers to a delegate, the performance of which remains subject to oversight by the authority which assumes full responsibility for the decisions of the delegate. According to the Court, in the latter situation no ‘true’ delegation takes place’.

⁴⁸ Jacopo Alberti, *op. cit.*, p. 375.

⁴⁹ C-9/56, *Meroni & Co., Industrie Metallurgiche, SpA v High Authority of the European Coal and Steel Community*, para. 150.

⁵⁰ Merijn Chamon, “A Constitutional Twilight Zone: EU Decentralized Agencies’ External Relations”, *Common Market Law Review*, No. 56, 2019, pp. 1509-1548, p. 1524, p. 1521.

⁵¹ Merijn Chamon, 2016, *op. cit.*, p. 255.

⁵² Dariusz Adamski, “The European Securities and Markets Authority Doctrine: A Constitutional Revolution and Economics of Delegation”, *European Law Review*, Vol. 6, No. 39, pp. 812-834. The notion of ‘precisely delineated’ can be summarised in three main points: first, the delegation of powers shall be exceptional; second, the agency’s powers must be embedded in a decision-making procedure involving other actors, and third the agency must pursue pre-defined criteria – see Merijn Chamon and Valerie Demedts, “Constitutional limits to the EU agencies’ external relations”, *TARN Working Paper*, No. 11, 2017, pp. 1-22. Marta Simoncini, 2016, *op. cit.*, p. 31, argues that:

‘[i]t can be inferred therefore that the ‘clearly defined executive powers’ that can be delegated are all those necessary administrative powers that exclude priority-setting, must conform to pre-determined criteria and are subject to supervision and judicial review [...] This framework outlines the very nature of administrative powers, which do not automatically exclude some degree of (administrative) discretion proportionate to the task to be performed, but necessarily preclude the exercise of legislative choices’.

TFEU Union bodies, offices, and agencies are clearly entitled to adopt acts of general application, which tears down the wall built up by *Romano* with the expression “acts having force of law”. Thus, the CJEU confirmed that the executive powers transferred to another body could have general or individual scope⁵³. According to Prof. Alberti, the ‘prohibition of discretionality’ should no longer be interpreted in absolute terms, but should be perceived as an ‘institutional clause’ to be applied on a case-by-case basis, according to the need⁵⁴. Moreover:

- In the *Short Selling* case⁵⁵ the relationship between EU agencies and Articles 290 and 291 TFEU was questioned as the CJEU opened the way for the adoption of a *tertium genus* of acts delegable to EU agencies⁵⁶. Scholars opposed this interpretation, taking into account the fact that the Court referred to the ‘delegation of such powers’⁵⁷. Excluding a “third way” for the attribution of powers to EU agencies would limit the degree to which EU sources were atypical and fragmented, as the powers of EU agencies would have the same nature as those established under Article 290 and/or Article 291 TFEU⁵⁸. On the other hand, while containing EU agency powers within these two norms, this interpretation will also limit the enhancement of EU agencies in the future and, with it, their contribution to the integration process that, in Prof. Alberti’s words, is in any case ‘sufficiently valid to allow agencies to respond to current exigences of the integration process’⁵⁹.

⁵³ C-270/12, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*, para. 66.

⁵⁴ Jacopo Alberti, *op. cit.*, p. 383.

⁵⁵ See the Opinion of Advocate General Jääskinen, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*, para. 86.

⁵⁶ David Fernández Rojo, *EU Migration Agencies: The Operation and Cooperation of FRONTEX, EASO and EUROPOL*, 2021, *op. cit.*, p. 170: ‘The core of the Meroni doctrine, that wide discretionary powers whose exercise entails a policy choice shall not be delegated, still survive as a parallel delegation system to Articles 290 and 291 TFEU’.

⁵⁷ C-270/12, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*, para. 78.

⁵⁸ Jacopo Alberti, *op. cit.*, p. 348.

⁵⁹ *Ibid.*, p. 351, and Augusto J. Piqueras García, “Legalidad y legitimidad en la actividad legislativa de la Unión europea”, in Diego Javier Liñán Noguerras and Pablo Jesús Martín Rodríguez, *Estado de Derecho y Unión Europea*, Madrid, Tecnos, 2018 pp. 313-344, p. 333. Although acceptable, such a theory finds in practice huge obstacles because of the multiple blurred lines that exist between delegated and implementing powers: even if delegated and implementing acts are conceptually different – the former having a quasi-legislative nature, the latter an executive one – they get confused in the practice and the choice of one or the other one is negotiated during the dialogues. See the critics made by Paz Andrés Sáenz de Santa María, “El Estado de derecho en el sistema institucional de la Unión europea: Realidades y desafíos”, in Diego Javier Liñán Noguerras and Pablo Jesús Martín Rodríguez, *op. cit.*, pp. 129-156, and Eljalil Tauschinsky and Wolfgang Weiß, *The Legislative Choice Between Delegated and Implementing Acts in EU Law: Walking in a Labyrinth*, Cheltenham, Edgar Elgar Publishing, 2018.

- The doctrine on the choice of the legal basis/es underpinning the EU agencies' legislation delimits the *quantum* and *quomodo* of the delegated powers⁶⁰. Although the establishment of an agency is an EU exclusive competence, its tasks and powers should be exercised according to the underlying EU competence and the principles governing its exercise. Therefore, the choice of a specific EU policy based on one or several legal basis/es conditions the exercise of the relevant EU competence and, consequently, its further delegation. The principles of necessity, proportionality and, where the competence is shared between the EU and its Member States, the principle of subsidiarity, shall be taken into account when it comes to evaluating the limits circumscribing EU agencies' activities⁶¹.
- The principle of institutional balance aims at preserving the institutional structure of the EU set forth by the founding Treaties⁶² – i.e., the distribution of powers among the institutions – which is tightly connected to the principle of loyal cooperation⁶³. Specifically, each institution: has the necessary independence in exercising its powers; must respect the powers of the other institutions; and may not unconditionally assign its powers to other institutions and bodies⁶⁴. According to Hillion, the prohibition on delegating powers to private parties was an additional requisite of the *Meroni* doctrine provided that the potential delegation breached the principle of institutional balance⁶⁵. In *Romano*, the Administrative Commission of the European Communities on Social Security for Migrant Workers⁶⁶ was a public body regulated on the basis of the TEEC legislation⁶⁷ – and not the TECSC – and it

⁶⁰ Jacopo Alberti, *op. cit.*, pp. 332 ff.

⁶¹ Marta Simoncini, *op. cit.*, p. 40.

⁶² Merijn Chamon, 2016, *op. cit.*, p. 249 ff. From p. 258 onward, the author reflects on the principle of institutional balance and its relationship with the principle of separation of powers. The author recognises that although functionally distinguished, in the EU the legislative and executive powers are not institutionally divided. Prof. Chamon states that these powers are fragmented: the legislature is made of three institutions, two of them composing a bicameral Parliament, and the executive, instead, is a “triade” made of the European Commission, the Council, and the Member States. Yet, two other phenomena contribute to its fragmentation: comitology and agencification, with the sole difference that only the former is recognised in the Treaties – see also Koen Lenaerts and Amayllis Verhoeven, “Institutional Balance as a Guarantee for Democracy in EU Governance”, in Christian Joerges and Renaud Dehousse, *op. cit.*, pp. 35-88.

⁶³ C-9/56, *Meroni & Co., Industrie Metallurgiche, SpA v High Authority of the European Coal and Steel Community*, para. 153, and Paz Andrés Sáenz de Santa María, *op. cit.*, pp. 129-156.

⁶⁴ Giandomenico Majone, “Delegation of Regulatory Powers in a Mixed Polity”, *European Law Journal*, Vol. 8, No 3, 2002, pp. 319-339, p. 327.

⁶⁵ Christophe Hillion, “Conferral, Cooperation, Balance in EU External Action”, in Marise Cremona, *Structural Principles in EU External Relations Law*, Portland, Hart Publishing, pp. 117-174.

⁶⁶ C-98/80, *Giuseppe Romano and Institut National d'Assurance Maladie-Invalidité*, para. 10.

⁶⁷ Article 80 of Regulation (EEC) No 1408/71 of the Council of 14 June 1971 on the application of social security schemes to employed persons and their families moving within the Community, *OJL* 149, 5.7.1971, pp. 2-50.

was conferred powers by the legislator (the Council) through an act of secondary law⁶⁸ in a manner similar to Union agencies.

1.2. The conclusion of administrative agreements and arrangements

As a manifestation of their legal personality⁶⁹, Union agencies cooperate with other institutions, bodies, and organs. Among other activities⁷⁰, EU agencies conclude administrative instruments that are variously labelled as agreements, arrangements, working arrangements, Memorandum of Understanding (MoU), and so on. Administrative instruments are challenging from a legal perspective⁷¹ as their nature and binding/soft law character⁷² must be assessed on

⁶⁸ Article 107 of Regulation (EEC) No 574/72 of the Council of 21 March 1972 fixing the procedure for implementing Regulation (EEC) No 1408/71 on the application of social security schemes to employed persons and their families moving within the Community, *OJ L* 74, 27.3.1972, pp. 1-83.

⁶⁹ It has been advanced that EU agencies benefit of a sort of limited or derived and functional international legal personality that empowers them to conclude international treaties. The clearest indication of EU agencies' ability to undertake negotiations internationally would be given by the conclusion of headquarters agreements which is accepted as a manifestation of EU agencies' international legal personality – see Gregor Schusterschitz, "European Agencies as Subjects of International Law", *International Organizations Law Review*, Vol. 1, 2004, pp. 163-188. Yet, basic principles stemming from the delegation doctrine contradict the possibility to confer on EU agencies international subjectivity: even when agencies are sufficiently empowered to act externally, they benefit of a degree of autonomy that cannot be equalised to full independence from the delegating institutions, bodies, and offices. As a general rule, EU agencies lack international subjectivity or, which is the same, that their personality depends on the international organisation within which they are established so that headquarters Agreements are concluded on its behalf – see Juan Santos Vara, *La gestión de las fronteras exteriores de la UE: Los nuevos poderes de la Agencia Frontex*, Valencia, Tirant Lo Blanch, 2021, p. 81 ff.; Merijn Chamon, 2019, "A Constitutional Twilight Zone: EU Decentralized Agencies' External Relations", *op. cit.*, p. 1524; Jacopo Alberti, *op. cit.*, p. 444 ff.; Florin Coman-Kund, "The International Dimension of the EU Agencies: Framing a Growing Legal-Institutional Phenomenon", *European Foreign Affairs Review*, Vol. 23, No. 1, 2018, pp. 97-118; Paula García Andrade, 2015, *op. cit.*, pp. 111-112; Andrea Ott, Ellen Vos, and Florin Coman-Kund, 2014, *loc. cit.*, and Andrea Ott, Ellen Vos, and Florin Coman-Kund, "EU agencies and their international mandate: A new category of global actors?", *Centre for the law of the EU external relations Working Paper*, No. 7, 2013, pp. 1-38, p. 14. In these terms, Union agencies must always act "under the umbrella" of the EU, though before intense controversies in the literature, the most prudent solution suggests adopting a case-by-case analysis in which each agency's decisions, resolutions, and practice are taken into account.

⁷⁰ Florin Coman-Kund, "The International Dimension of the EU Agencies: Framing a Framing Legal-Institutional Phenomenon", *European Foreign Affairs Review*, Vol. 23, No. 1, 2018, pp. 97-118, p. 99:

'First, EU agencies become involved in the management of the external dimension of their respective policy area by assisting the EU institutions and the Member States in their relations with third countries and international organizations. Second, third countries and international organizations participate in the internal structures of some EU agencies. Third, EU agencies establish direct cooperation with third countries or third country authorities and international organizations materialized most importantly through the conclusion of arrangements or agreements'.

⁷¹ Antonio Pastor Palomar, "Efectos de los Acuerdos internacionales en el derecho de la UE: práctica reciente y perspectiva desde España", in José María Beneyto Pérez, *Tratado de Derecho y Políticas de la Unión Europea. Tomo IX. Acción Exterior de la UE*, Navarra, Thomson Reuters Aranzadi, 2017, pp. 81-132.

⁷² Especially because of the increasing agreement of soft-law instruments by the EU with third partners in the AFSJ and, specifically, in the migration field – see Juan Santos Vara, "Soft international agreements on migration with third countries: a challenge to democratic and judicial controls in the EU", in Sergio Carrera, Juan Santos Vara, and Tineke Strik, *Constitutionalising the External Dimensions of EU Migration Policies in Times of Crisis: Legality, Rule of Law and Fundamental Rights Reconsidered*, Cheltenham, Edward Elgar Publishing, 2019, pp. 21-38, p. 23, recalling for example the EU-Turkey Statement of 18 March 2016 available at www.consilium.europa.eu, and the Joint Way Forward on migration issues between Afghanistan and the EU of 2 October 2016 available at www.asyl.at.

a case-by-case basis while taking into account the wording, content, and context of the agreement⁷³ – i.e., the non *nomen omen* rule applies. However, discerning a binding agreement from non-binding arrangements is of prime importance since the former may encroach upon Article 218 TFEU as long as the Council of the EU keeps a monopoly over the EU’s treaty-making power. Similarly, Prof. Alberti highlights that soft law instruments may impact the EU’s external relations⁷⁴ and warns not to rely on the “arrangements” formula, as these instruments may only be formally non-binding and, consequently, turn out to be relevant in light of Article 218 TFEU.

Union agencies’ external actions are limited by two main sets of principles:

- firstly, those that stem from the EU external action⁷⁵ – including the theory on implied competences, where this is relevant⁷⁶ – to justify the necessity of an external engagement to achieve the internal mandate, and
- secondly, those that integrate the revised *Meroni* doctrine.

Therefore, the administrative agreements concluded by Union agencies should be separated from those international treaties that public international law labels as “administrative” since these are negotiated with a simplified procedure⁷⁷, in the absence of a diplomatic intermediary and according to the domestic rules of a state or an organisation⁷⁸. In the EU legal order, there

⁷³ C-327/91, *French Republic v Commission of the European Communities*, para. 15. Yet, we unknowledge that the terms ‘arrangement’ in EU law suggests that the instrument has a non-binding character according to the European Commission, Vademecum on the external action of the European union, SEC(2011) 881/3, Brussels, 21 September 2012, p. 52.

⁷⁴ Jacopo Alberti, *op. cit.*, p. 440: ‘[...] it would be a mistake not to take account of this whole set of international agreements because of their *soft-law* character; there would be a risk of underestimating legal instruments which, in any case, can create commitments on the part of the Union and have effects at international level’ (the translation is ours).

⁷⁵ See Chapter II.

⁷⁶ *Ibidem*.

⁷⁷ The national Parliament is usually not involved in the proceeding, which is left in the hands of the government because of its technical competence and non-political content. Andrea Ott, “The EU Commission’s administrative agreements: “delegated treaty-making” in between delegated and implementing rule-making”, in Eljalill Tauschinsky and Wolfgang Weiß, *op. cit.*, pp. 200-232, p. 211, finds that the majority of states assign to their national Parliament the conclusion of those treaties that affects their constitutions while leaving to the ‘[...] the national executive, acting through government, ministries and state agencies, addresses the general management of relations with third countries and international organisations’. The latter case happens, for example, when the state decides to implement an existing agreement. However, its executive nature does not escape the application of international law: it is still a treaty binding upon the state.

⁷⁸ Fred L Morrison, “Executive Agreements”, in Anne Peters and Hélène Ruiz Fabri, *Max Planck Encyclopedias of International Law*, New York, Oxford University Press, 2019. See also: José Martín y Pérez de Nanclares, “La ley de tratados y otros acuerdos internacionales: una nueva regulación para disciplinar una práctica internacional difícil de ignorar”, *Revista Española de Derecho Internacional*, Vol. 67, No. 1, 2015, pp. 13-60, p. 40 ff., and Article 2(b) of the Ley 25/2014, de 27 de noviembre, de Tratados y otros Acuerdos Internacionales, *Boletín Oficial del Estado* No. 288, of 28.11.2014, specifying that an international administrative agreement is (the translation is ours):

‘[...] an agreement of an international character not constituting a treaty which is concluded by organs, agencies or entities of a subject of international law which are competent in relation to the subject-matter, the conclusion of which is provided for in the treaty which it executes or implements, the usual content of which is of a technical nature whatever its name and which is governed by international law. An international

is no such a provision: the possibility to conclude a treaty in a “simplified” form is mentioned, for example, in Article 218(7) TFEU for which the Council may ‘[...] authorize the negotiator to approve on the Union’s behalf modifications to the agreement where it provides for them to be adopted by a simplified procedure or by a body set up by the agreement. The Council may attach specific conditions to such authorisation’. This is an exceptional rule that confirms that the Council maintains the monopoly on the EU’s treaty-making power – namely, the opening of the negotiations, the signature, and the conclusion of the treaty⁷⁹ – for both political and technical agreements. The European Commission, instead, is in charge of negotiating international treaties with third countries and international organisations⁸⁰ to ‘ensure the Union’s external representation’⁸¹. This strict interpretation has been confirmed by the CJEU, notably, not only for binding treaties⁸² but also for soft law examples⁸³. Yet, unlike a Council of the EU delegation to the European Commission, the delegation of external competences to a decentralised Union agency is more complex if it is considered that not only the Council of

administrative agreement is not an international administrative agreement concluded by the same organs, bodies, agencies or entities when it is governed by an internal legal order’.

According to the author, p. 45 (our own translation):

‘From the external perspective, it seems clear that International Administrative Agreements are governed by international law, can give rise to international legal obligations and their breach can give rise to state responsibility. So far they are no different from treaties. However, from a domestic perspective, it does not seem simple to maintain their supra-legal nature with regard to their normative rank, when their internal processing has been left out of the parliamentary process derived from Articles 93 and 94.1 of the Constitution. [...] It is assumed, therefore, that if the International Administrative Agreements has been correctly concluded within the (formal and material) limits set by the treaty on which it is based, it would in any case be that treaty which could come into collision with an internal norm of a legal nature and, with regard to it, there is no doubt of its accepted supra-legal status’.

⁷⁹ ‘The Council shall authorize the opening of negotiations, adopt negotiating directives, authorise the signing of agreements and conclude them’.

⁸⁰ Article 218(3) TFEU that also contemplates the High Representative of the Union for Foreign Affairs and Security Policy in case the agreement concerns these policies.

⁸¹ Article 17 TEU.

⁸² C-327/91, *French Republic v Commission of the European Communities*, paras. 25-30, where the CJEU analysed the validity of a binding instrument on competition law concluded by the European Commission autonomously with the US: While the European Commission alleged that it was competent to conclude it, given that it was an administrative agreement for which the European Community’s liability would have not been triggered in case of an international claim, the CJEU opposed this. Yet, the CJEU did not clarify whether the European Commission could have been delegated the power to conclude such an international treaty, but if this was the case, with the Council as the principal and the European Commission as the delegated authority, the *Meroni* doctrine should have been applied.

⁸³ C-233/02, *French Republic v Commission of the European Communities*, para. 42, where the CJEU found that the Guidelines on Regulatory Cooperation and Transparency concluded by the European Commission with the US did not bind the contracting parties and that in no way had the European Commission restricted its own competence on making legislative initiatives. In these terms, the CJEU supported the European Commission to conclude non-binding agreements on behalf of the EU provided that: first, it acted within the policy framework dictated by the Council and, second, it respected the principle of institutional balance. However, in C-660/13, *Council of the European Union v European Commission*, 28 July 2016, EU:C:2016:616, the CJEU sentenced that the European Commission could, on behalf of the EU, sign the 2013 Addendum attached to the 2006 MoU establishing the Swiss Confederation’s commitment to providing a financial contribution to new Member States accessing the EU since this fell within the European Commission’s executive and management functions sealed under Article 17(1) TEU.

the EU, but also the European Commission's, the European Parliament's, and the CJEU's competences must be respected⁸⁴. Theoretically, the Council could authorise the agency to act on the EU's behalf '[...] in which case special attention is required to ensure that the prerogatives of the Commission and Parliament are safeguarded, otherwise the Council would be circumventing the institutional balance transpiring from Article 218 TFEU'⁸⁵.

Despite this, the Common Approach on decentralised agencies agreed between the European Parliament, the Council of the EU and the European Commission in 2012⁸⁶ has prevented Union agencies having any power to act on the EU's behalf both in terms of representation – which corresponds to the European Commission – and of its political commitment – which is a Council prerogative⁸⁷. Therefore, there can be no clash between the Union agencies and the EU Council as there may be between the European Commission and the EU Council in the external layer, as Union agencies can in no way act on behalf of the EU⁸⁸. Such an interpretation confirms that Union agencies' external actions are limited to so-called "technical-administrative" agreements or arrangements, being that their implementation is concluded under Article 218 TFEU or as implementation of EU legislation⁸⁹. The Common Approach also added that:

⁸⁴ For the European Commission see: C-73/14, *Council of the European Union v European Commission*, EU:C:2015:663, para. 58, and C-425/13, *Commission v Council (Australia emissions trading system)*, EU:C:2015:483, para. 88. For the European Parliament see C-263/14, *Parliament v Council (Tanzania)*, EU:C:2016:435, para.70.

⁸⁵ Merijn Chamon, 2019, "A Constitutional Twilight Zone: EU Decentralized Agencies' External Relations", *op. cit.*, p. 1519.

⁸⁶ See the Council of the EU, *Evaluation of European Union agencies Endorsement to the Joint Statement and Common Approach*, 1450/12, Brussels, 18 June 2012. Emphasising the role of the CJEU and the *ex ante* control over international agreements is Jacopo Alberti, *op. cit.*, p. 441.

⁸⁷ Council of the EU, 1450/12, Brussels, 18 June 2012, para. 25: 'This strategy and appropriate working arrangements with partner DGs in the Commission should ensure that the agencies operate within their mandate and the existing institutional framework, and that they are not seen as representing the EU position to an outside audience or as committing the EU to international obligations'.

⁸⁸ Merijn Chamon, 2019, "A Constitutional Twilight Zone: EU Decentralized Agencies' External Relations", *op. cit.*, p. 1528: 'By providing that EU agencies can never act on behalf of the EU any institutional balance concerns are pre-empted, since the prerogatives of the EU institutions as enshrined in Article 218 TFEU are safeguarded. If an agency acts on its own behalf, it cannot thwart the prerogatives of the EU institutions'.

⁸⁹ Apart from *ad hoc* delegation by virtue of Articles 290-291 TFEU, implementing powers are conferred to the European Commission under Articles 17 TEU and 220 TFEU. Thus, the European Commission's executive powers sealed under Article 17(1) TEU – 'It shall ensure the application of the Treaties, and of measures adopted by the institutions pursuant to them' – does not authorise it to implement international agreements *tout court*. This Article maintains that the European Commission must "ensure" the application of the law, but does not confer it implementing competences. These are indeed regulated under Article 291(2) TFEU for which: 'Where uniform conditions for implementing legally binding Union acts are needed, those acts shall confer implementing powers on the Commission, or, in duly justified specific cases and in the cases provided for in Articles 24 and 26 of the Treaty on European Union, on the Council'. Therefore, both internally and externally, the European Commission must be conferred implementing powers in an act of secondary law – i.e., a legislative measure or an international agreement. Article 220 TFEU, instead, allows the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy to implement the instruments of cooperation sealed with the organs of the United Nations and its specialised agencies, the Council of Europe, the Organisation for Security (OSCE) and the OECD. Despite controversies, we believe that Article 220 TFEU does not confer to the EU any specific empowerment but recalls that the European Commission and the High Representative of the Union for Foreign

- Union agencies must lay out their external strategy for their annual or multi-work programs, including specifications on resources and the principles and modalities of any international cooperation;
- the strategy and working agreements concluded with the relevant European Commission's Director General must ensure that it acts within its mandate and the existing institutional framework⁹⁰;
- any specific initiative must be subject to approval by the Union agency's Management Board, and
- the Union agency, the European Commission and the relevant Director General must be informed of the international activity of the former so as to supervise its consistency with the laws surrounding EU external action.

The Common Approach has been criticised from at least two angles: first, because it failed to agree on the European Parliament's democratic oversight on the exercise of administrative external powers – especially when the agreement or arrangement envisaged touches sensitive domains, among which human rights stands out⁹¹; second, the control exercised by the European Commission over the Union agency's strategy and working agreements is not satisfactory as, if the latter acts outside its mandate and the existing institutional framework, the European Commission cannot compel it to respect its boundaries. Provided that the majority of decentralised agencies are established through an act of secondary law, it is not clear why the European Commission alone is in charge of ensuring their compliance⁹². As Prof. Chamon notes, this uncertainty (as well as numerous additional points of confusion) will not be resolved until the position of Union agencies within the EU administrative apparatus and, specifically, their relationship with the European Commission, the European Parliament, the Council of the EU, and the Member States is clarified⁹³. For this reason, the studies conducted so far on EU

Affairs and Security Policy are conferred implementing – and not discretionary – powers when the EU acts in that specific legal framework.

⁹⁰ European Commission, *Vademecum on the external action of the European union*, SEC(2011)881/3, Brussels, 21 September 2012, p. 18.

⁹¹ Juan Santos Vara, "The External Activities of AFSJ Agencies: The Weakness of Democratic and Judicial Controls", *European Foreign Affairs Review*, Vol. 20, No. 1, 2015, pp. 115-136, and Id., "Análisis del marco jurídico-político de la dimensión exterior de las agencias del espacio de libertad, seguridad y justicia", in Montserrat Pi Llorens and Esther Zapater Duque, *La dimensión exterior de las agencias del espacio de libertad, seguridad, y justicia*, Madrid, Marcial Pons Ediciones Jurídicas y Sociales, 2014, pp. 9-34, p. 10.

⁹² This would not be the case when it is clear that the agreement or arrangement falls within the European Commission's competence, as it is the case of Article 220(2) TFEU conferring to it and to the High Representative of the Union for Foreign Affairs and Security Policy the implementation of agreements concluded with international organisations. In parallel, this disposition imposes to the Council of the EU not to override such a European Commission's prerogative.

⁹³ Merijn Chamon, 2019, "A Constitutional Twilight Zone: EU Decentralized Agencies' External Relations", *op. cit.*, p. 1536.

descentralised agencies – that we are part of – follow an empirical approach that scrutinises each specific agency’s agreement or arrangement and the underlying legal framework, that is, the degree of participation of each specific institution⁹⁴.

2. The European Union Agency for the operational management of large-scale IT systems in the Area of Freedom, Security and Justice: eu-LISA

2.1. The progressive empowerment of eu-LISA

In 2009, the European Commission delegated⁹⁵ the operational management of the three existing large-scale IT systems – namely the SIS II, the Eurodac⁹⁶ and the VIS – to a new EU agency⁹⁷: eu-LISA. The agency was meant to be a centre of excellence in the field of development and management of large-scale IT systems. It was intended that it executes the activities linked to the development and the operations of the central part of the systems, including the uniform interfaces in the Member States and the related networks. This should have allowed most of the setbacks that the European Commission suffered when developing the SIS II and the VIS to be avoided⁹⁸ although, in reality, the implementation of the new generation of large-scale IT systems and of the interoperability components is delaying too⁹⁹. By restoring the trust of the Member States in the EU’s IT capacities, the establishment of eu-LISA marked a crucial passage for the management of large-scale IT systems, which was sufficient to allow for the adoption of legislative reforms that had failed up until that point, this included the long-awaited interoperability package¹⁰⁰.

⁹⁴ See, for example, Andrea Ott, Ellen Vos, and Florin Coman-Kund, 2013, *loc. cit.*, who emphasise how the three following elements must be taken into account: first, the nature of the (executive) power delegated; second, the amount of control that the delegating authority can exercise over the delegate and, third, the actual exercise of the powers.

⁹⁵ The European Commission was responsible of the operational management of the SIS II and the VIS during a “transitional period” of no more than five years according to Article 15(4) of Regulation (EC) No 1987/2006 and Article 6(4) of the VIS Regulation.

⁹⁶ As amended by the 2013 Eurodac recast Regulation.

⁹⁷ See the Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, *OJ L* 286, 1.11.2011, pp. 1-17 (eu-LISA 2011 Regulation hereinafter), that was repealed by the eu-LISA 2018 Regulation.

⁹⁸ Council of the EU, *ANNEX Legislative financial statement to the Proposal for a Regulation of the European Parliament and the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*, 14082/16 ADD 1, Brussels, 16 November 2016, p. 16.

⁹⁹ Council of the EU, *Implementation of interoperability: state of play and revised timeline*, 14947/21, Brussels, 13 December 2021.

¹⁰⁰ Aden Hartmut, “Interoperability Between EU Policing and Migration Databases: Risks for Privacy”, *European Public Law*, Vol. 26, No 1, 2020, pp. 93-108, p. 97: ‘While the physical IT infrastructure remains in Strasbourg in a unit now belonging to eu-LISA, bundling the governance of major parts of the EU’s IT infrastructure for the AFSJ in a single agency is not only a step towards more coherent governance of the databases but also facilitates the implementation of interoperability’.

2.1.1. The negotiations surrounding the establishment and succession of eu-LISA

Although the discussions held by the Member States' delegations within the Council of the EU on this first instrument are largely either not, or only partially, accessible, from the negotiations of the first eu-LISA Regulation it can be inferred that the provision of a new EU agency for the operational management of IT systems was welcomed by the majority of the EU community¹⁰¹. The necessity to delegate the management of the systems to a decentralised agency had been already advanced in the planning of the second generation SIS. At that time, the steering committee was perceived as the ideal solution, where the EU institutions and the Member States could be gathered to decide the strategic and operational management of the systems¹⁰². The EDPS supported the idea of establishing a responsible and autonomous authority in the IT field so as to avoid a liability vacuum¹⁰³. Nevertheless, this choice should have been accompanied by a clear allocation of human resources enabling the agency to perform its tasks and accomplish its goals, which might not be the case with eu-LISA that, despite the inflation of its mandate in recent years, is still one of the AFSJ's smallest agencies¹⁰⁴. However, not all delegations blindly welcomed the establishment of eu-LISA. The German delegation questioned the added value brought by a new agency and asked the European

¹⁰¹ See the Council of the EU, *Submission of the Work Programmes 2012 and 2013 of the Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 6401/13, Brussels, 28 February 2013, p. 36, according to which 'The creation of the Agency is situated in the political context of the Stockholm programme and the action plan implementing this programme, which set the framework for the EU's response to major challenges in this policy area and outline a number of key developments in border management and security over the forthcoming period'. Concretely, the Work Programme refers to the economic crisis and the political challenges that stroke the EU in the early 2000s, especially the flogging number of migrants in the EU, that called for the efficient implementation of new political strategy supported by the use of new technologies.

¹⁰² See the Council of the EU, *Development of the Schengen Information System II and possible synergies with a future Visa Information System (VIS)*, 16106/03, Brussels, 15 December 2003, p. 22, that excluded the possibility to pass the strategic management – i.e. the decision making part – of the SIS from the Council to the European Commission as '[...] it is highly unlikely that strategic management of a system, the only users of which are Member States and authorised participating States, would be entrusted to the Commission only, even if assisted by a committee'.

¹⁰³ See Article 340 TFEU for which the EU institutions shall be responsible for contractual non-accomplishments and non-contractual damages and Article 32 of the eu-LISA 2018 Regulation. Furthermore, the Agency's decisions are subjected to the European Ombudsman and the CJEU according to Article 114(5) and 119 of the same Regulation. The report on the financial management of the year is sent to the Commission's Accounting Officer and the European Court of Auditors by 1 March of the following years – see the Council of the EU, *Submission of the 2011 Activity Report of the Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 12913/12, Brussels, 25 July 2012.

¹⁰⁴ See the eu-LISA, *Consolidated Annual Activity Report 2020*, Tallin, 29 June 2021, p. 55 ff., available at www.eulisa.europa.eu: 'The year 2020 was extremely challenging for eu-LISA in terms of human resources. First, it was the first year after the completion of the Agency's structural transformation, i.e. 'eu-LISA 2.0', the preparation for the cultural transformation programme, as well as defining and launching of the Leadership Development Programme. Second, the COVID-19 pandemic created numerous unprecedented situations for eu-LISA staff. Due to the pandemic, the Agency swiftly rearranged its working modalities, keeping in mind not only the business continuity but also the possible impact of the changes in work environment on the well-being of the staff'.

Commission to lay down its tasks in detail¹⁰⁵. This delegation called on the principles of necessity, proportionality, and subsidiarity to justify the establishment of a new agency while discarding other options ‘[...] in terms of deregulation, subsidiarity, proportionality (cost-benefit analysis) and concentration’¹⁰⁶.

In reality, before proposing the establishment of the new agency, the European Commission studied different means of moving forward on the management of large-scale IT systems, among which it contemplated the possibility to: further engage the Member States’ authorities, or enlarging the operational mandate of the EBCG Agency, or that of Europol. However, the empowerment of the EBCG Agency or of Europol was rejected as, according to the European Commission, this would have increased the risks of misuse of personal data¹⁰⁷. Besides, while the EBCG Agency rested on a hybrid competence with one foot in the freedom area and the other one in the PJCCM, it was clear that Europol’s mandate fell short of managing the VIS and the Eurodac. Opting for a regulatory agency established through the ordinary legislative procedure and acting under the democratic scrutiny of the European Parliament would have better safeguarded the respect of the EU data protection legislation instead of relying on the Member States’ authorities.

Thus, eu-LISA absorbed the operational functions of the European Commission for the implantation of centralised systems in the AFSJ¹⁰⁸. The 2009 Proposal contemplated a package made of two instruments according to the inter-pillars structure sealed by the Treaty of Maastricht in 1992¹⁰⁹: on the one hand, a Regulation would have formed the basis for the legal

¹⁰⁵ A similar position was maintained by Austria in the Council of the EU, *Comments on the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 12870/09, Brussels, 2 September 2009.

¹⁰⁶ Council of the EU, *German comments on the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 14212/09, Brussels, 9 October 2009, p. 1.

¹⁰⁷ Confront the Commission Staff Working Document accompanying document to the Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice and Proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty, COM(2009) 293 final, Brussels.

¹⁰⁸ See Articles 3 to 5 of the eu-LISA 2011 Regulation. Already in the SIS II and the VIS the Management Authority was depicted as responsible for the operational management of the systems after a transitional period of maximum five years in which the European Commission was still in charge of these tasks – see Article 15 of the Council Decision 2007/533/JHA and Article 26 of the VIS Regulation.

¹⁰⁹ See the Council of the EU, *Communication from the Commission Legislative package establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 11709/09, Brussels, 3 July 2009. Indeed, the freedom of movement dispositions were communitarised under the first pillar in 1997 by the Treaty of Amsterdam, while the norms on the police cooperation and judicial cooperation in the criminal field would have belonged to the third pillar under Title VI of the TEU until the entry into force of the Treaty of Lisbon.

framework of SIS II, VIS, and Eurodac with regard to the first pillar aspects¹¹⁰; on the other hand, a Decision would have regulated the SIS and the VIS as far as the third-pillar structure was concerned¹¹¹. Provided that no legal basis in the founding Treaties sufficiently empowered the EU to act¹¹², the Proposal was underpinned by the SIS II, the VIS, and the Eurodac legal bases, and specifically: Articles 62(2)(a), 62(2)(b)(ii), 63(1)(a), 63(3)(b) and Article 66 of the 2002 TEC; and Article 30(1)(a) and (b), and Article 34(2)(c) of the 2002 TEU¹¹³. Under this complex legal framework, eu-LISA was called on to facilitate communication and cooperation between the Member States' administrations and would have been technically supported by the EU policies underpinning the three systems involved. On closer inspection, the legal framework was missing a reference to Article 31(1)(a) and (b) of the 2002 TEU on criminal judicial cooperation regarding the relevant SIS II alerts¹¹⁴. Such an exclusion was justified by the need to successfully gather compatible legal bases for the adoption of a unique decision of the Council following its unanimous vote. In parallel, a Council regulation could have been adopted under the co-decision procedure, as Article 66 of the 2002 TEC had shifted from unanimity to qualified majority voting¹¹⁵.

The entry into force of the Lisbon Treaty marked a crucial passage for the AFSJ and the communitarisation of the policies underpinned therein. The EDPS pointed out that Articles 77(1)(b), 77(2)(b), 77(2)(a), 78(2)(e), 79(2)(c) and 74 TFEU were the corresponding valid legal bases for the proposed regulation that should have been adopted under the ordinary legislative procedure. Provided that Articles 30(1)(a) and (b), and 34(2)(c) of the 2002 TEU corresponded to the new Articles 87(2)(a) and 87(3) TFEU, the underlying law-making procedures were found to be incompatible with each other. The EDPS highlighted how measures under Article 87(3) TFEU on the adoption of legislative texts on operational cooperation between police forces could be adopted only under a special legislative procedure with the unanimity in the EU

¹¹⁰ See the Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, COM(2009) 292 final, COM(2009) 294 final, Brussels, 24.6.2009.

¹¹¹ *Ibidem*.

¹¹² Among others, see the CJEU in on the Cartagena Protocol on Biosafety to the Convention on Biological Diversity, *U.N.T.S.* Vol. 2226, p. 208, signed in Montreal on 29 January 2000, entered into force on 11 September 2003, that is *Opinion 2/00*.

¹¹³ On the operational cooperation of law enforcement authorities, the collection, storage, processing, analysis and exchange of relevant information, and on the empowerment of the EU Council to adopt any decision that shall exclude any approximation of the national legislations.

¹¹⁴ Recalling that the SIS II was established on the basis of Articles 62(2)(a) and 63(3)(b) of the 1997 TEC; the VIS on the basis of Article 62(2)(b)(ii) of the 1997 TEC, and the Eurodac on Article 63(1)(a) of the 1997 TEC.

¹¹⁵ See the Protocol on Article 67 of the Treaty establishing the European Community, *OJ C* 325, 24.12.2002, p. 184, for which: 'From 1 May 2004, the Council shall act by a qualified majority, on a proposal from the Commission and after consulting the European Parliament, in order to adopt the measures referred to in Article 66 of the Treaty establishing the European Community'.

Council and after consulting the European Parliament¹¹⁶; on the contrary, Articles 87(2)(a) TFEU on the measures concerning the collection, storage, processing, analysis, and exchange of relevant information fell under the ordinary procedure. The EDPS suggested opting for the most communitarised legal basis – namely 87(2)(a) TFEU – since:

‘[...] the use of the ordinary legislative procedure implies the full involvement of the European Parliament and ensures democratic legitimacy of the proposal. [...] According to the EDPS, taking Article 87(2)(a) TFEU as the sole legal basis would have enabled the merging of the two current proposals into a single instrument to be adopted in accordance with the ordinary legislative procedure’¹¹⁷.

Implicitly, the EDPS was recognising that the proposed eu-LISA regulation overflowed the Schengen *acquis* while focusing on freedom, security and justice matters. Otherwise, Article 87(3) TFEU could have been considered compatible with Article 87(2)(a) TFEU¹¹⁸. Moreover, and with Article 74 TFEU aimed at expanding to the whole Title V of the TFEU since 2009, this legal basis was no longer limited to the freedom of movement area and could now embrace PJCCM too¹¹⁹. The use of Article 74 TFEU in place of legal bases (more tightly) anchored to the intergovernmental framework was firstly experimented with in the eu-LISA 2009 Proposal. In March 2010, the European Commission submitted a new Proposal welcoming the EDPS’ observations¹²⁰ and underpinned it with the following legal bases: Articles 77(2)(a) and (b), 78(2)(e), 79(2)(c), 74, 82(1)(d), and 87(2)(a) TFEU. The legal framework was revised following suggestions by the Legal Service of the Council of the EU that integrated Articles 85(1) and 88(2) TFEU to signal the presence of the EU agencies, that is, Eurojust and Europol respectively¹²¹.

Soon after operations started, the European Commission advanced some new suggestions to expand its mandate following the evaluation of eu-LISA’s activities between 2012-2015. The evaluation was taken as the basis to revise the agency’s mandate in 2017, knowing that the

¹¹⁶ Recalling that Article 87(3), first paragraph, TFEU sets forth: ‘The Council, acting in accordance with a special legislative procedure, may establish measures concerning operational cooperation between the authorities referred to in this Article. The Council shall act unanimously after consulting the European Parliament’. Yet, Article 87(3) TFEU also allows the establishment of an enhanced cooperation in case the unanimity cannot be reached.

¹¹⁷ See the Council of the EU, *Opinion of the EDPS - on the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and - on the proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty*, 5039/10, Brussels, 7 January 2010, p. 4.

¹¹⁸ ‘The specific procedure provided for in the second and third subparagraphs shall not apply to acts which constitute a development of the Schengen *acquis*’.

¹¹⁹ See also Article 76 TFEU referring to Chapters 4 and 5 of Title V TFEU.

¹²⁰ See the Council of the EU, *Amended Proposal for a Regulation (eu) no .../... of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 8151/10, Brussels, 30 March 2010.

¹²¹ See Article 4B in the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice - Preparation for the high-level trialogue*, 7638/11, Brussels, 11 March 2011, p. 5.

adoption of the legislative package regarding the last generation of large-scale IT systems and interoperability was coming¹²². The 2011 Regulation was then repealed in 2018 with a new regulation that designates a “new” eu-LISA as the successor of the existing one¹²³.

2.1.2. The enhancement of eu-LISA’s mandate

The core task of eu-LISA consists of the operational management of large-scale IT systems and the availability of information that must flow twenty-four hours a day, seven days a week. However, from 2011 onward, the range of eu-LISA’s competences under the concept of ‘operational management’ was questioned. Although both the Council of the EU and the European Parliament found that eu-LISA’s ‘operational tasks’ should have included all tasks necessary to keep large-scale IT systems functioning in accordance with the legal instruments governing each of these systems, the latter also wanted to delegate the responsibility of managing the communication infrastructure used by the IT systems while excluding the possibility of their interoperability to eu-LISA¹²⁴. The agency was finally assigned the communication infrastructure tasks too ‘[...] in order to protect it from threats and to ensure the security of the communication infrastructure and of the IT systems, including data exchanged through it’¹²⁵.

In this sense, the operational activity of eu-LISA encompasses the provision of ‘[...] an appropriate level of data and physical security, in accordance with the applicable rules, including specific provisions for each large-scale IT system’¹²⁶, but it does not touch the content of the data¹²⁷. These tasks are developed through encryption techniques that allow the processing of data while preventing the unauthorised reading, copying, modification, or deletion of personal data¹²⁸. However, while in its first Regulation, the European Commission remained responsible for the contractual and budgetary aspects of the communication

¹²² Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011*, 10820/17, Brussels, 30 June 2017.

¹²³ See Article 53 of eu-LISA 2018 Regulation.

¹²⁴ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Open issues – Preparation of the informal trilogue*, 14469/10, Brussels, 25 October 2010, p. 23.

¹²⁵ *Ibid.*, p. 26.

¹²⁶ See Article 2(g) of eu-LISA 2018 Regulation.

¹²⁷ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Compromise version*, 16282/09 ADD 4, Brussels, 20 November 2009.

¹²⁸ See Article 11 of eu-LISA 2018 Regulation. See also the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Possible agreement with the EP*, 10827/11, Brussels, 30 May 2011.

infrastructure of the systems under the Trans-European Services for Telematics between Administrations network of the European Commission Directorate General for Informatics (DIGIT)¹²⁹, these competences were delegated to eu-LISA in 2018¹³⁰. The sole exception concerns those systems that are held in the EuroDomain – namely the Eurodac and the ECRIS-TCN – whose communication infrastructure, including operational management and security elements, were to be divided between the agency and the European Commission¹³¹. This implies relatively discretionary powers for the agency in choosing its partners – including external private-sector entities or bodies¹³² – to which it delegates the communication infrastructure in accordance with Article 36(2) of the Commission Regulation (EC, Euratom) 2343/2002¹³³. Consequently, the EDPS raised some concerns regarding the scope of eu-LISA's mandate and asked for further clarification on the activities the agency was undertaking.

First of all, in 2009 the EDPS complained about the lack of a definition of large-scale IT system. Although the three systems at issue shared some common features – including the coexistence of a centralised system assigned to the European Commission and a national interface of the Member States' competence – the lack of a clear definition put into question the limits of the agency's activities. The Article 29 DPWP gave some indications on what 'large-scale' processing of data means on the assumption that this kind of operation requires the establishment of a Data Protection Officer¹³⁴. In this sense, the Article 29 DPWP identified four main characteristics:

- the number of individuals/data subjects concerned – either as a specific number or as a proportion of the relevant population;
- the volume of data and/or the range of different data items being processed;
- the duration, or permanence, of the data processing activity, and
- the geographical extent of the processing activity.

However, the eu-LISA 2011 Regulation did not consider these points and other networks that do not share these characteristics have been included under eu-LISA's competence since

¹²⁹ The Trans-European Services for Telematics between Administrations (TESTA-ng) is operated and financed by the European Commission so that no contractual tasks or budget is transferred to eu-LISA.

¹³⁰ See Article 11 of eu-LISA Regulation of 2018 and the Council of the EU, *Report from the Commission to the European Parliament and the Council on the functioning of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA)* Council of the European Union, 10873/17, Brussels, 3 July 2017, p. 4.

¹³¹ Article 11(1) of eu-LISA 2018 Regulation.

¹³² Among others, the US company Deloitte is actively contributing to the implementation of the large-scale IT systems and the interoperability package.

¹³³ Commission Regulation (EC, Euratom) No 2343/2002 of 23 December 2002 on the framework Financial Regulation for the bodies referred to in Article 185 of Council Regulation (EC, Euratom) No 1605/2002 on the Financial Regulation applicable to the general budget of the European Communities, *OJ L 357*, 31.12.2002, pp. 72-90. See Article 7(5) of the eu-LISA 2011 Regulation.

¹³⁴ See the Guidelines of the Article 29 DPWP on *Data Protection Officers ('DPOs')*, Brussels, 13.12.2016, p. 21.

2011. First of all, the DubliNet and the VISION¹³⁵ that are not databases, but communication channels integrating the main systems of Eurodac and VIS respectively. These were delegated to the agency through inter-service consultation without amending the relevant Regulation¹³⁶. Besides, the 2018 Regulation confers on eu-LISA the management of new IT systems whose characteristics recall SIS II, Eurodac and VIS's architectures – like EES, ETIAS, and ECRIS-TCN – which leaves the door open for the agency's empowerment thanks to the adoption of new legislative measures. In this sense, the computerised system for cross-border communication in civil and criminal proceeding (e-CODEX) was included within eu-LISA's mandate¹³⁷. Yet, the eu-LISA 2018 Regulation is not provided with any legal basis delegating to it competences in the civil judicial jurisdiction field, which seriously questions its incorporation¹³⁸. Also, the European Commission announced in April 2022 to have mandated the agency the elaboration of a platform for digitally registering the refugees fleeing the war in Ukraine and pooling Member States' reception data, 'which does not require a new legal basis'¹³⁹ despite its obvious humanitarian overtones. It must be noted that if the European Commission's Proposals for a Prüm II Regulation¹⁴⁰ and for a collaboration platform to support joint investigations teams¹⁴¹ will be adopted, eu-LISA will be assigned further responsibilities: the former, provides for the design and development of a "router" interconnecting the Member States and Europol's databases to query, retrieve and score biometric data; the latter, requires the elaboration of both centralised and decentralised components to facilitate the exchange of electronic communication, information, and evidence, including large amounts of data, among members and participants of joint investigation teams. However, the proposals of the European

¹³⁵ See Articles 6, 7 and 8 respectively of eu-LISA 2018 Regulation.

¹³⁶ The former between the Agency and DG HOME, the latter between the Member States and Iceland, Liechtenstein and Norway which puts into question what the EDPS stand out according to the Council of the EU, 10820/17, Brussels, 30 June 2017, p. 3.

¹³⁷ See recital (18) eu-LISA 2018 Regulation, and the Proposal for a Regulation of the European Parliament and of the Council on a computerised system for communication in cross-border civil and criminal proceedings (e-CODEX system), and amending Regulation (EU) 2018/1726, COM(2020)712 final, Brussels, 2.12.2020. In March 2022, Member States had already aligned their position within the EU Council according to "Feu vert des États membres à l'installation du système informatique e-CODEX à Tallinn", *Bulletin Quotidien Europe*, No 12767, 23.7.2021, while the European Parliament has given its approval as announced in "Le PE approuve l'accord interinstitutionnel sur le règlement 'e-CODEX'", *Bulletin Quotidien Europe*, No. 1291, 25.3.2022.

¹³⁸ "Accord PE/Conseil de l'UE sur le transfert du système informatique e-CODEX au siège de l'agence eu-LISA", *Bulletin Quotidien Europe*, No 12850, 10.12.2021: 'The e-CODEX system allows different national justice systems to be digitally interconnected in order to carry out cross-border proceedings in civil and criminal matters. Its users (judicial authorities, lawyers, citizens) can send and receive electronically documents, legal forms or evidence in a fast and secure way' (our own translation).

¹³⁹ "La plateforme d'enregistrement des déplacements de réfugiés ukrainiens dans l'UE ne sera pas prête avant fin mai", *Bulletin Quotidien Europe*, No. 12935, 21.4.2022.

¹⁴⁰ Article 65 of the Proposal for a Prüm II Regulation.

¹⁴¹ Proposal for a Regulation of the European Parliament and of the Council establishing a collaboration platform to support the functioning of Joint Investigation Teams and amending Regulation (EU) 2018/1726, COM(2021) 756 final, Brussels, 1.12.2021.

Commission to delegate to eu-LISA the management of archiving False and Authentic Documents Online (FADO)¹⁴² and to host the system for registration and monitoring, as well as the allocation mechanism for applications for international protection advanced by the Eurodac 2016 Proposal were rejected¹⁴³. From our perspective, even if the scope of the agency's activities seems to embrace the whole AFSJ – concretely Articles 67 to 89 TFEU¹⁴⁴ – the concept of a “large-scale IT system” should be clarified in order to precisely delineate the agency's empowerment and, specifically, to elucidate which kind of IT systems falls within the agency's mandate¹⁴⁵. In its absence, such a blurred definition may justify the absorption of decentralised systems, too. Indeed, the new 2018 Regulation establishes that eu-LISA can assist the Member States in the implementation of decentralised databases – like the Prüm, the API, and the PNR¹⁴⁶ – provided that they are implemented under Union law¹⁴⁷. This shall be carried out through an enhanced cooperation request from a group of four Member States, with the prior approval of the European Commission and a positive decision from the Management Board. The EDPS opposed such a delegation to eu-LISA in the lack of any express provision in the underlying legislative measures regulating the decentralised systems at stake¹⁴⁸. Further, the EDPS opposed the possibility to delegate these tasks through a delegated act as proposed during the negotiations. This expedient would have almost certainly circumvented the democratic scrutiny guaranteed by the ordinary legislative procedure through which the agency's mandate must be amended.

Moreover, although the eu-LISA 2018 Regulation clarifies that Member States remain competent for the national part of the systems, this assumption is shaped in light of the extended

¹⁴² See recital (15) of the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011 – Third revised draft*, 13128/17, Brussels, 23 October 2017.

¹⁴³ See Article 44 of eu-LISA 2018 Regulation. See the positions of The Netherlands and Poland in the Proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011, Brussels, 29.6.2017.

¹⁴⁴ See recital (18) of eu-LISA 2018 Regulation.

¹⁴⁵ In these terms, we hope that the analysis conducted in Chapter III will be helpful.

¹⁴⁶ In the cases of API and PNR, the Regulation clearly defines what eu-LISA shall do ‘[i]n such a case the Agency shall centrally collect the data from air carriers and transmit those data to the Member States via the common component or router’ – see Article 16(4), second paragraph, of eu-LISA 2018 Regulation.

¹⁴⁷ See Article 16(4) of eu-LISA 2018 Regulation and the negotiations on Article 12 of the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011 – Revised draft*, 11884/17, Brussels, 13 September 2017.

¹⁴⁸ Council of the EU, *Opinion of the European Data Protection Supervisor on the Proposal for Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011*, 13188/17, Brussels, 13 October 2017, p 10.

tasks delegated to eu-LISA in providing advice and support. eu-LISA has been empowered to provide support to the Member States for the implementation of their own national components¹⁴⁹ since it contributed to enhancing the capacity of Eurodac in the Greek hotspot and because of its intervention in the EU regional task forces deployed in Piraeus and Catania¹⁵⁰. Thus, the 2018 Regulation allows the Member States to ask the European Commission for eu-LISA's support in connecting their national systems to the central ones. In case of extraordinary needs related to security or migration, this request may be addressed directly to the agency which will report it to the Management Board and it will ultimately be monitored by the European Commission through the annual activity report. Such an empowerment blurs the original subdivision of competences between eu-LISA and the Member States, where the agency was only responsible for managing the centralised infrastructure. The discussions held during the negotiations within the Council of the EU show that Member States are quite reluctant to entrust eu-LISA with their operational competences and jealously guard the data stored in the systems as their own – though the fact that the information is made available to other States – as well as for the quality of the data contained therein¹⁵¹. The German delegation called for delineation between the competences of the agency and the Member States:

‘[i]t should be emphasized that the Agency's primary competence is limited to central European information systems and not to systems or system components, which are the responsibility of [Member States]. The future negotiations will clarify the extent to which the targeted support for individual [Member States] results in a transfer of responsibilities for operation and development from the national systems of the respective [Member States] to the Agency. At the present time, however, a strict separation of competences between the individual [Member States] and eu-LISA must be observed’¹⁵².

As the EDPS observed, the gathering of the IT systems' management under eu-LISA's umbrella of competences facilitated the establishment of their interoperability¹⁵³. The eu-LISA 2018 Regulation provides for an explicit competence on the interoperability and its wide formulation seems to include not only the interoperability Regulations (EU) 817 and 818 of

¹⁴⁹ See Article 16 of eu-LISA 2018 Regulation.

¹⁵⁰ See the Council of the EU, 10873/17, Brussels, 3 July 2017, p. 9.

¹⁵¹ See the comment from The Netherlands on the quality of the data in Council of the EU, 11884/17, Brussels, 13 September 2017, p. 8. Recalling Thierry Balzacq, Didier Bigo, Sergio Carrera, and Elspeth Guild, “Security and the Two-Level Game: The Treaty of Prüm, the EU and the Management of Threats”, *Centre for European Policies Studies Working Document*, No. 234, Brussels, 2006, pp. 1-28, p. 15: ‘Data exchange represents a form of knowledge that increases the state's power. Thus, authorities that hold that data are anxious to retain control over that data’.

¹⁵² Council of the EU, 11884/17, Brussels, 13 September 2017, p. 4.

¹⁵³ See Article 13 of the eu-LISA 2018 Regulation. For example, eu-LISA is delegated the publication of the lists of competent authorities with access to the large-scale IT systems and the correspondent notifications are available in its official webpage at <https://www.eulisa.europa.eu>. The latest reports were published in the *OJ* on the 16 July 2021 for SIS II and on the 9 March 2021 for the Eurodac.

2019 in the terms analysed hereafter, but also the infra-system connections set forth in the specific regulations concerning each IT system. The EDPS was not against such a project, but it clarified that interoperability could only be possible with respect to the data protection principles, especially that of purpose limitation, and that the European Commission could have delegated such an empowerment only after the adoption of the relevant legislation – i.e., it could have not delegated the interoperability of large-scale IT systems *sine tempore*. Meanwhile, no interconnection should have been implemented. The European Commission asked the agency to create a pilot scheme for the future development of the IO Regulations – the so-called Smart Borders Pilot¹⁵⁴ – that was assigned to the agency with an infra-institutional delegation agreement. Yet, the pilot scheme that the agency had to develop for the European Commission was also questioned by the EDPS as it did not clarify under which conditions the agency should have carried it out¹⁵⁵. Notably, the eu-LISA 2018 Regulation also extends pilot projects to basic acts to test the feasibility of an action and its usefulness¹⁵⁶, without it being limited to Article 54(2) of the financial Regulation¹⁵⁷, which allows the agency to plan and implement testing activities for the systems. As the EDPS recalled in its Opinion on the 2016 Eurodac recast Proposal, biometric data cannot be anonymised, since fingerprints and facial images always make the identification of individuals possible¹⁵⁸. Therefore, identity data should not be used for testing purposes. In any case, the possibility to delegate the creation of pilot projects to the agency highlighted wider problems according to the non-delegation theory: the German delegation alleged that former Article 202 of the 2002 TEC authorised the Council to delegate implementing, but not legislative, powers. In its words:

¹⁵⁴ “eu-LISA and EC signed the Delegation Agreement on Smart Borders Pilot”, *Press Release*, 16 January 2015, available at www.eulisa.europa.eu.

¹⁵⁵ See Article 9 of eu-LISA 2011 Regulation.

¹⁵⁶ As the French delegation recalls, pilot projects are the result of the development in research referred to in Article 8 of eu-LISA 2018 Regulation – see the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 14995/09, Brussels, 27 October 2009, p. 4. According to the Ad Hoc Group on Information Exchange, pilot projects should be elaborated on the basis of the end-users needs which requires the constant involvement of the Member States’ authorities – see the *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice - input based on the Information Management Strategy*, 14838/09, Brussels, 26 October 2009.

¹⁵⁷ Article 15 of eu-LISA 2018 Regulation.

¹⁵⁸ See the Council of the UE, *Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European criminal records information system (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011 - Revised text following COPEN meeting on 11 and 12 September 2017*, 12187/17, Brussels, 19 September 2017, p. 15.

‘Authorising the Commission to carry out pilot projects for large-scale IT systems under Title IV of the EC Treaty and Title VI of the Treaty on European Union goes beyond mere implementation and is therefore impermissible’¹⁵⁹.

Thus, the creation of pilot projects was perceived as a law-making activity that rested with the Council and could not be delegated to the European Commission, being that the latter was only entitled to adopt implementing measures.

Finally, and although the eu-LISA Regulations expressly mentioned the capacity to develop new IT systems¹⁶⁰, the EDPS recalled that the preparation, development, and monitoring of new systems, as well as their interoperability, should derive from new legislation proposals submitted by the European Commission and adopted under the ordinary legislative procedure as they would widen the agency’s mandate. The European Parliament, for its part, stressed the need to expressly refer to a specific and separated empowerment based on Title V of the TFEU ‘[...] following an impact assessment and taking into account the developments in research referred to in Article 5 and the results of pilot schemes referred to in Article 6’¹⁶¹.

2.2. eu-LISA’s structure and organisation

2.2.1. The choice of eu-LISA’s headquarters and seats

The establishment of eu-LISA’s seat gave rise to widespread discussions among the Member States’ delegations within the Council of the EU¹⁶². Among others, the fact that the EBCG Agency had not signed its headquarters agreement when the European Commission had advanced its first Proposal was taken into account when considering whether to delegate operational management of the systems to it¹⁶³. From the very beginning, France supported the establishment of eu-LISA’s headquarters in Strasbourg, provided that the C-SIS had already been located there and that the VIS would be added later; only the Eurodac was located in the European Commission’s premises in Luxembourg and Brussels. In its letter, France explains

¹⁵⁹ See the Council of the EU, 16282/09 ADD 4, Brussels, 20 November 2009 (26.11), p. 4.

¹⁶⁰ See Article 1(3) of the eu-LISA 2011 Regulation, and Article 1(4) of eu-LISA 2018 Regulation.

¹⁶¹ See the Council of the EU, 14469/10, Brussels, 25 October 2010, p. 25, and today recital (18) of eu-LISA 2018 Regulation.

¹⁶² See, for example, the Council of the EU: *Legislative package establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Location of the seat of the Agency*, 13305/09, Brussels, 15 September 2009, and the *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Draft compromise text*, 8269/10, Brussels, 7 April 2010, p. 7.

¹⁶³ Council of the EU, *Commission staff working document accompanying document to the - Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice and - Proposal for a Council decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty - Impact assessment*, 11709/09 ADD 2, Brussels, 3 July 2009, p. 22.

that although in the Presidency Conclusion it was agreed to ‘give priority to Acceding States, once they have joined the Union, in the distribution of the seats of other offices or agencies to be set up in the future’¹⁶⁴, a single location with a back-up should have been preferred. According to the French, the establishment of eu-LISA in Strasbourg would have provided for:

- ‘operational continuity and preservation of the know-how acquired in the development and operation of the SIS over almost fifteen years;
- creation of synergies: bringing together management, planning and operational activities at a single site, which is one of the reasons for turning it into agency;
- security: the Strasbourg site has proved its capability;
- budgetary rationality: existing investment is safeguarded. The choice of a single site for planning and operation allows much expenditure on travel and telecommunications to be avoided and development synergies to be created’¹⁶⁵.

In addition, France alleged that the decentralised management of large-scale IT systems contradicted the European Commission proposal aiming at ‘[...] providing for the operational management of these systems in one entity, benefiting from economies of scale, creating critical mass and ensuring the highest possible utilisation rate of capital and human resources’¹⁶⁶. Similarly, the Hungarian delegation pointed out that a back-up site should have been established for security reasons, but it opposed moving the systems’ location while warning that a decentralised administration might have resulted in additional costs and organisational overhead¹⁶⁷. The United Kingdom, for its part, objected¹⁶⁸ to the insertion of criteria related to the “services” provided by the host state to determine the choice of the seat of the new agency,

¹⁶⁴ Council of the EU, *Brussels European Council \ 12 and 13 December 2003 presidency conclusions*, 5381/04, Brussels, 5 February 2004, p. 27.

¹⁶⁵ Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – seat of the Agency*, 5038/10, Brussels, 7 January 2010.

¹⁶⁶ Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Compromise version*, 16282/09 ADD 3, Brussels, 20 November 2009, pp. 5 and 6. The Austrian and the German delegations shows their agreement in not decentralising the Agency’s seats apart from the necessity of pointing out a back-up site. See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Revised compromise version*, 5747/10 ADD 1, Brussels, 1 February 2010, and the *German comments on the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 9802/10, Brussels, 17 May 2010.

¹⁶⁷ Council of the EU, *Comments on the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 14609/09, Brussels, 16 October 2009, p. 2. A similar approach was highlighted by the German delegation in Council of the EU, 16282/09 ADD 4, Brussels, 20 November 2009, p. 4, and by the Austrian delegation in the Council of the EU, 5747/10 ADD 1, Brussels, 1 February 2010, p. 2.

¹⁶⁸ Council of the EU, 14995/09, Brussels, 27 October 2009, p. 7: ‘The location of the headquarters is a political decision to be taken by the ministers and the inclusion of this kind of criterion here with regard to the host Member State would prejudice that decision. The last sentence in the paragraph should accordingly be deleted’.

since this might have caused an unwanted precedent. This also explains why the eu-LISA 2018 Regulation not only sets forth that the host Member State must provide the accommodation and facilities to eu-LISA's members, as well as to members of their families, but it also foresees that they shall furnish multilingual, European-oriented schooling, and appropriate transport connections to the agency for its proper functioning¹⁶⁹ as originally proposed for the 2011 Regulation. Yet, because of the insertion of such criteria, the United Kingdom voted against the 2011 Regulation¹⁷⁰: In its view, the choice of an agency's seat should have remained a political choice to be adopted by unanimity in the Council¹⁷¹ and in no case should the eu-LISA Regulations have set a precedent¹⁷². In these terms, the CJEU's forthcoming judgment on the 'migration' of the European Medicine Agency and the European Labour Authority seats will be decisive¹⁷³. In it, the CJEU will have to clarify whether the Council decision concerning the establishment of the seat of an agency is an EU act or not, and whether such a decision must be underpinned by Article 341 TFEU, or by an EU act adopted by ordinary legislative procedure¹⁷⁴.

¹⁶⁹ Article 30 of eu-LISA 2018 Regulation.

¹⁷⁰ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (first reading) – Adoption of the legislative act = Statements*, 13136/2/11 REV 2 ADD 1, Brussels, 9 September 2011: 'Through its vote, the UK reaffirms its view and reiterates the position set out in the Council declaration that: · The location of EU Agencies should continue to be made by common accord of the Representatives of the Governments of the Member States; and · The inclusion of this text does in no way constitute a precedent for deciding on the seats of EU Agencies in the future'.

¹⁷¹ Reference was made to Article 341 TFEU for which: 'The seat of the institutions of the Union shall be determined by common accord of the governments of the Member States'. It was supported also by the Austrian delegation in Council of the EU, 5747/10 ADD 1, Brussels, 1 February 2010, p. 2, that extended the reference of this legal basis for the choice of the backup location.

¹⁷² See the Council of the EU: *Proposal for a Regulation of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 10827/2/11, REV 2 ADD 1, Brussels, 8 June 2011, and the *Proposal for a Regulation of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 10827/2/11, REV 2 ADD 3, Brussels, 8 June 2011.

¹⁷³ See the Opinion of Advocate General Bobek, C-59/18 and C-182/18, *Italian Republic (C-59/18) Comune di Milano (C-182/18) v Council of the European Union*, 6 October 2021, EU:C:2021:812, and C-106/19 and C-232/19, *Italian Republic (C-106/19) Comune di Milano (C-232/19) v Council of the European Union*, 6 October 2021, EU:C:2021:816. Specifically, in C-106/19 and C-232/19 the municipality of Milan challenged the Regulation (EU) 2018/1718 of the European Parliament and of the Council of 14 November 2018 amending Regulation (EC) No 726/2004 as regards the location of the seat of the European Medicines Agency Text with EEA relevance, PE/40/2018/REV/1, OJ/L 291, 16.11.2018, pp. 3-4, for not having properly involved the European Parliament in the ordinary legislative procedure and for descending from an unlawful decision adopted by the Council of the EU establishing the agency's seat.

¹⁷⁴ From the time being, the Opinion of Advocate General Bobek, C-59/18 and C-182/18, *Italian Republic (C-59/18) Comune di Milano (C-182/18) v Council of the European Union*, paras. 82 and 108, has come to the conclusion that the decisions at stake are not acts of the EU or dissimulating the Council of the EU's decisions, but they are acts adopted by the own Member States' representatives; consequently, the Court has no competence to assess their validity by virtue of Article 263 TFEU as they have no juridical effect in the EU legal order. However, the Advocate General maintains that the establishment of an agency's seat should be adopted by the Council and the European Parliament following a European Commission's proposal according to the ordinary law-making procedure and not by the Member States' agreement.

Following the Estonian and French's candidacies to host the new agency's seat¹⁷⁵, eu-LISA was spread across three different Member States: the seat is located in Tallin (Estonia)¹⁷⁶; the technical site for the operational management of the systems is in Strasbourg (France)¹⁷⁷, and the back-up site is in Sankt Johann im Pongau (Austria). The tripartite location required the conclusion of three agreements: a headquarters agreement with Estonia, and two site agreements with France and Austria respectively¹⁷⁸. While the headquarters in Tallin was completely furnished with a new 'EU-House' for eu-LISA, the accommodation in France was rearranged on the basis of the existing C-SIS site. The back-up site is expected to host eu-LISA's personnel only in case of a disaster preventing the agency from operating in Strasbourg which, in any case, required the enhancement of the previously prepared establishment. Among others, the tripartite site of eu-LISA justified the nomination of a Deputy Executive Director¹⁷⁹. Although during the tripartite negotiations the European Parliament suggested realising a cost-benefit assessment before establishing the seat of the new-born agency and to facilitate its long-term functioning¹⁸⁰, its suggestion was not incorporated in the 2011 Regulation. Not surprisingly, the eu-LISA financial report also confirms that the merging of the agency's sites would be beneficial: 'It is likely that management effectiveness could be increased and administrative costs reduced if all staff were centralised in one location'¹⁸¹.

¹⁷⁵ See the Council of the EU: *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice - seat of the Agency*, 5285/10, Brussels, 13 January 2010; 14469/10, Brussels, 25 October 2010, p. 3, and the *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice - seat of the Agency*, 17287/10, Brussels, 1 December 2010. The documents reveal that the European Parliament supported the choice of a unique seat plus a back-up one too. It also accepted the delegations' choice in agreeing it with the unanimous vote in the Council of the EU.

¹⁷⁶ See the "eu-LISA Site Agreement ratified by the Estonian Parliament", *Press Release*, 18 February 2015 and the "eu-LISA Headquarters Now in a Smart New House", *Press Release*, 19 September 2018, available at www.eulisa.europa.eu.

¹⁷⁷ See recital (5) and Article 17 of eu-LISA 2018 Regulation. The France's and Estonia's offers to host the Agency are available in Council of the EU, 11709/09, Brussels, 3 July 2009, p. 5, and 5285/10, Brussels, 13 January 2010 – see the "eu-LISA signs Site Agreement with France", 5 December 2013 and the "eu-LISA Inaugurates Its Operational Site's New Building", *Press Release*, 20 November 2018, available at www.eulisa.europa.eu.

¹⁷⁸ Council of the EU, 6401/13, Brussels, 28 February 2013.

¹⁷⁹ Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011 – Outcome of the European Parliament's first reading (Strasbourg 2 to 5 July 2018)*, 10714/18, Brussels, 12 July 2018, p. 21. Note that eu-LISA became financially autonomous from the European Commission on 22 May 2013.

¹⁸⁰ Council of the EU, 7638/11, Brussels, 11 March 2011, p. 44: 'In order to ensure the best possible long-term functioning of the agency, a cost-benefit assessment shall precede the conclusion of the headquarters Agreement. Particular account shall be taken of a Member State's willingness and ability to provide its own resources to host the Agency in such a way as to ensure its smooth establishment and operation'.

¹⁸¹ Council of the EU, *Report on the annual accounts of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) for the financial year 2013 together with the Agency's replies*, 16479/14, Brussels, 5 December 2014.

The evaluation conducted by the European Commission attached to its 2017 Proposal found that: ‘The additional direct and indirect costs linked to the multi-site arrangement of the Agency are therefore considered justified and reasonable’¹⁸². However, it also clearly affirms that the Estonian location was chosen for ‘political considerations’ that produced superfluous costs.

- Tangible costs are caused by the mission costs for travel between sites, parallel procedures for procurement, and the use of multiple contractors for service provision – e.g., cleaning, security – or missed opportunities for economies of scale in running costs.
- Intangible disadvantages include negative impacts on the fluidity of communication between sites, which are further compounded by the functional divide between Tallinn and Strasbourg; inherent management challenges imposed by geographical distance; retaining and attracting skilled labour, and the impediment to the emergence of a strong and unified organisational culture.

2.2.2. eu-LISA’s governance

The governance structure of eu-LISA was revised in 2018 to allow the utmost participation of the Member States in the European Commission’s operational activity. Their participation addressed and lessened the national governments’ hostilities against the agency’s enhanced empowerment, given that Member States were involved in the decision-taking process. First and foremost, the Management Board gathers the European Commission and the Member States’ representatives in order to agree policy task forces and to control the agency’s activity¹⁸³. eu-LISA’s Management Board is made of one representative from each Member State and two representatives from the European Commission¹⁸⁴. The decisions are taken by majority¹⁸⁵ of all its members, including all Member States bound by any legislative instrument governing the development, establishment, operation and use of a large-scale IT system – i.e., the United Kingdom, Ireland, and Denmark if they have transposed the relevant regulation in their national law¹⁸⁶ – while Schengen Associated Countries have been kept in an ambiguous position¹⁸⁷. The Management Board is assisted by the annual activity of the Advisory Groups

¹⁸² Council of the EU, 10873/17, Brussels, 3 July 2017, p. 5.

¹⁸³ See Article 19 of eu-LISA 2018 Regulation.

¹⁸⁴ See Article 20 of eu-LISA 2018 Regulation. The eu-LISA 2011 Regulation already foresaw such a composition in its Article 13.

¹⁸⁵ However, during the negotiations some delegations proposed to use a three-quarter majority. See for example the Dutch position in Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Compromise version*, 16282/09 ADD 7, Brussels, 3 December 2009, p. 5.

¹⁸⁶ See Article 20(4) of eu-LISA 2018 Regulation.

¹⁸⁷ See Article 42(2) of the eu-LISA 2018 Regulation: ‘Under the relevant provisions of the agreements referred to in paragraph 1, arrangements shall be made specifying, in particular, the nature and extent of, and the detailed

through which experts from the Member States actively participate in the agency's activities¹⁸⁸. The Advisory Groups include: the SIS II Advisory Group; the VIS Advisory Group; the Eurodac Advisory Group; the EES-ETIAS Advisory Group, and any other advisory group relating to a large-scale IT system when provided for in the relevant Union legal act governing the development, establishment, operation, and use of the large-scale IT system in question. In addition, an Interoperability Advisory Group has been gathered: according to Article 75 of the IO Regulations, the Interoperability Advisory Group should meet regularly until the interoperability component begins operations and should submit reports to the Programme Management Board after each meeting. It shall provide the technical expertise to support the tasks of the Programme Management Board and follow up on the Member States' level of preparation¹⁸⁹. Despite criticism regarding the proliferation of technical groups and their impact on transparency and efficiency¹⁹⁰, eu-LISA's advisory groups did not replace the existing committees established for the systems¹⁹¹. Besides, the agency is fully autonomous and it has its own representative: the Executive Director¹⁹². Although the Austrian delegation proposed to keep the eu-LISA Executive Director's appointment under the Council's competence following the Europol's model¹⁹³, the Executive Director is appointed by the Management Board for a term of five years and is chosen from a list of eligible candidates identified in an open competition organised by the European Commission¹⁹⁴. Moreover, the 2018 Regulation stipulated that the agency appoint the following: A Data Protection Officer; a Security Officer, and an Accounting Officer¹⁹⁵.

rules for, the participation of countries as referred to in paragraph 1 in the work of the Agency, including provisions on financial contributions, staff and voting rights'. Indeed, these countries asked specifically to suppress the provision that prevented them to vote *tout court* – see the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Compromise version*, 16282/09 ADD 1, Brussels, 20 November 2009, p. 2: 'According to this original wording, the associated states would not be able to vote on any type of decision relating to the IT- systems managed by the Agency, even though this kind of decisions regarding operational matters will have a direct impact on the competent authorities of the associated states and their tasks'. The answers forwarded by these countries detail how they financially contribute to the operational and installation of the systems – 5% for SIS II and 12% for Eurodac.

¹⁸⁸ See Article 27 of eu-LISA 2018 Regulation.

¹⁸⁹ Article 54(6), last paragraph, of the IO Regulations.

¹⁹⁰ See the Spanish and German's positions in Council of the EU, 16282/09 ADD 4, Brussels, 20 November 2009 (26.11).

¹⁹¹ As the Austrian delegation proposed in Council of the EU, 5747/10 ADD 1, Brussels, 1 February 2010, p. 7.

¹⁹² See Article 24 of eu-LISA 2018 Regulation. It is elected by the Management Board according to Article 25 of eu-LISA 2018 Regulation. Discussions on the procedure for the election of the Executive Director were held during the negotiations of the eu-LISA Regulation according to Council of the EU, 14469/10, Brussels, 25 October 2010.

¹⁹³ Austrian delegation in Council of the EU, 5747/10 ADD 1, Brussels, 1 February 2010, p. 5 ff.

¹⁹⁴ See Article 25 of eu-LISA 2018 Regulation.

¹⁹⁵ See Article 18 of eu-LISA 2018 Regulation.

2.2.3. Variable geometry in eu-LISA

Variable geometry has been a challenging topic in relation to the governance of eu-LISA and caused discussions during the negotiations of the Proposal of 2008, which was finally adopted in 2011.

The United Kingdom and Ireland's participation in the agency should have been limited to the scope of SIS II regarding law enforcement regulated under the Council Decision 2007/533/JHA and to the Eurodac¹⁹⁶. However, since the 2011 Regulation was finally merged into unique single legal text¹⁹⁷, the United Kingdom requested that it should take part in some of the dispositions of the Regulation by virtue of Article 4 of the Schengen Protocol No 19¹⁹⁸. The United Kingdom notified its intention to participate by virtue of Protocol No 21 to the freedom, security and justice dispositions concerning: the SIS II as governed by Regulation (EC) No 1987/2006, the VIS, the EES, and the ETIAS¹⁹⁹. In reality, Protocol No 21 clearly establishes that the United Kingdom could not adhere to the large-scale IT systems agreements falling within the "freedom area", unless it adhered to the underlying EU policy. Therefore, the United Kingdom was authorised by the Council to take part in the dispositions on the eu-LISA Regulation concerning the Schengen *acquis*²⁰⁰ with some nuances: despite affirming that 'the United Kingdom will not participate in the proposed Regulation on other grounds', the

¹⁹⁶ See Chapter V.

¹⁹⁷ Recital (13) of the Council Decision (EU) 2018/1600 of 28 September 2018 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis* relating to the European Union Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), ST/12040/2018/INIT, OJ L 267, 25.10.2018, pp. 3-5:

'The proposed Agency, as is the case for the Agency, should have a single legal personality and be characterised by the unity of its organisational and financial structure. To this end, the proposed Agency should be established by means of a single legislative instrument which should be voted on within the Council in its entirety. Moreover, once adopted, the proposed Regulation should become applicable in its entirety in the Member States bound by it. This excludes the possibility of partial applicability for the United Kingdom'.

¹⁹⁸ Protocol No 19, and See the Council of the EU, *Council Decision concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis relating to the establishment of a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 15766/10, Brussels, 23 November 2010.

¹⁹⁹ Council of the EU, *Notification from UK to participate in the adoption and application of the Council Decision authorising the opening of negotiations on an arrangement between the European Union, on the one part, and the Republic of Iceland, the Kingdom of Norway, the Swiss Confederation and the Principality of Liechtenstein, on the other part, on the modalities of the participation by those States in the European Agency for the operational management of large-scale information systems in the area of freedom, security and justice*, 12128/12, Brussels, 6 July 2012.

²⁰⁰ See the Council Decision 2010/779/EU of 14 December 2010 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis* relating to the establishment of a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 333, 17.12.2010, p. 58, and the Council Decision (EU) 2018/1600 of 28 September 2018 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis* relating to the European Union Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), ST/12040/2018/INIT, OJ L 267, 25.10.2018, pp. 3-5.

participation of the United Kingdom in the proposed Regulation ‘would be without prejudice to the fact that at present the United Kingdom does not and cannot participate in the provisions of the Schengen acquis relating to the free movement of third country nationals, visa policy and the crossing by persons of the external borders of the Member States’²⁰¹. Consequently, the formulation of recital (33) of eu-LISA 2011 Regulation was unusual, as it allowed the United Kingdom to take part in the provisions of the SIS II and the VIS, despite not taking part in the underlying fields of Union policies, by virtue of Article 1 of Council Decision 2010/779/EU of 14 December 2010. Also, this required that specific provisions were inserted so as to limit the United Kingdom’s voting rights in the eu-LISA Management Board. Specifically, Article 23(3) of the eu-LISA Regulation states that each member is entitled to vote if it is bound by the legal act governing the development, establishment, operation, and use of a large-scale IT system managed by the agency on a question which concerns that large-scale IT system. Ireland, however, was not willing to adhere to the dispositions of large-scale IT systems falling within the freedom section. Consequently, Ireland could not opt-in the eu-LISA Regulation²⁰², but it asked to take part in it with an ex-post notification letter²⁰³. As far as Denmark was concerned, it should have notified the European Commission within a period of six months whether it would adopt the relevant measure²⁰⁴.

Finally, the Schengen Associated Countries were allowed to participate in the eu-LISA Regulation, though an additional agreement was established²⁰⁵ in order to grant these states a status comparable to that of the Member States²⁰⁶. These countries are granted voting rights on decisions of an operational and technical nature and on opinions of the Advisory Groups concerning IT systems in which the associated countries participated, that is Dublin- and Eurodac-related matters, excluding the regulatory decisions of the agency²⁰⁷. The European

²⁰¹ See recitals (15) and (16) of the Council Decision (EU) 2018/1600 of 28 September 2018 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis relating to the European Union Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), ST/12040/2018/INIT, *OJ L* 267, 25.10.2018, pp. 3-5.

²⁰² According to recital (53) of the eu-LISA 2018 Regulation: ‘Since it is not possible, under these circumstances, to ensure that this Regulation is applicable in its entirety to Ireland, as required by Article 288 TFEU, Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application, without prejudice to its rights under Protocols No 19 and No 21’.

²⁰³ See the Council of the EU, *Request from Ireland to take part in the Regulation of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 8510/12, Brussels, 3 April 2012.

²⁰⁴ See recital (32) of eu-LISA Regulation of 2011.

²⁰⁵ See recitals (33) to (37) and Article 37 of the eu-LISA 2011 Regulation.

²⁰⁶ Council of the EU, *Council Decision authorising the opening of negotiations on an arrangement between the European Union, on the one part, and the Republic of Iceland, the Kingdom of Norway, the Swiss Confederation and the Principality of Liechtenstein, on the other part, on the modalities of the participation by those States in the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 11796/12, Brussels, 10 July 2012.

²⁰⁷ Article 42 of the eu-LISA 2018 Regulation.

Commission was against their participation by virtue of the principle of “institutional autonomy”, and suggested underpinning the agreement with Articles 218(3) and (4) TFEU alone²⁰⁸.

2.3. eu-LISA and the protection of personal data: The responsibility for the processing of personal data

Despite the enhancement of the agency in the fields of data protection, the eu-LISA 2018 Regulation was not underpinned by Article 16 TFEU, nor was an impact assessment conducted by an external evaluator, but by Ernst & Young²⁰⁹. During the negotiations of the EES Regulation, the German delegation highlighted that eu-LISA is the sole body that can guarantee the lawful processing of personal data, without either accessing rights to the data, or developing statutory decision-making powers²¹⁰. In its words:

‘The European Data Protection Supervisor has rightly described the Commission as a sui generis controller under data protection law vis-à-vis its responsibility for the operational management of large-scale IT systems and its leading role in their development and maintenance. While the role of controller covers much more than processing (in particular system development), it is more limited than that of an ordinary supervisory body because the Commission has no access to the personal data processed in large-scale IT systems’²¹¹.

In addition, the EDPS suggested that a reference to Article 16 TFEU was justified, at least as far as the monitoring activity was concerned.

Article 36 defines the purposes for which eu-LISA can process personal data:

- where necessary for the performance of its tasks related to the operational management of the large-scale IT systems entrusted to it under Union law, and
- where necessary for its administrative tasks.

²⁰⁸ See the Council of the EU, *Council Decision authorising the opening of negotiations on an arrangement between the European Union, on the one part, and the Republic of Iceland, the Kingdom of Norway, the Swiss Confederation and the Principality of Liechtenstein, on the other part, on the modalities of the participation by those States in the European Agency for the operational management of large-scale information systems in the area of freedom, security and justice, Common Guidelines Consultation deadline, 17 July 2012*, 11797/12, Brussels, 16 July 2012.

²⁰⁹ Council of the EU, *Commission staff working document executive summary of the commission staff working document eu-LISA evaluation Accompanying the document Report from the Commission to the European Parliament and the Council on the functioning of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA)*, 10873/17 ADD 2, Brussels, 3 July 2017.

²¹⁰ Which lastly questioned the validity of the establishment of a “regulatory agency” whose decision must be subjected to the annulment proceeding before the CJEU. See the Council of the EU, 14212/09, Brussels, 9 October 2009 (23.10), p. 9.

²¹⁰ The European Commission refers to Article 50 of the EES Regulation for recently agreed text in Council of the EU, 12187/17, Brussels, 19 September 2017.

²¹¹ Council of the EU, 14212/09, Brussels, 9 October 2009 (23.10).

Until today, it is not clear in which circumstances eu-LISA has access to the data and to what extent. The EDPS Opinion on the 2016 recast Eurodac Proposal stated that it should be clarified who has access to the data, including for testing purposes, especially when eu-LISA uses external contractors in light of the principle of confidentiality²¹². The preparation, development, and operational management of the systems requires eu-LISA to respect the data protection principles, first of all the principle of data protection by design and by default. Indeed, apart from its operational tasks, eu-LISA is responsible for a series of competences that ensure the respect of the EU legal framework in the field of the protection of personal data²¹³ with due consideration of the specific provisions governing each IT system²¹⁴.

eu-LISA is assigned crucial tasks during the design and development phases of the IT interoperability infrastructure²¹⁵, as well as – with certain questions regarding to its conformity with the *Short Selling* case²¹⁶ – competences to realise the necessary adaptations required to ensure interoperability in the large-scale IT systems and interoperability components including the CRRS²¹⁷. Along with its other responsibilities, eu-LISA is required to define the design and the evolution of the physical architecture of the interoperability components, including their communication infrastructures, and the technical specifications²¹⁸. The development and implementation of the interoperability components, instead, should follow the adoption of the relevant secondary legislations²¹⁹ and they ‘[...] shall consist of the elaboration and implementation of the technical specifications, testing²²⁰ and overall project management and coordination’²²¹. Moreover, eu-LISA plays a prominent role for the entry into force of the so-

²¹² See the Council of the EU, 12187/17, Brussels, 19 September 2017, p. 15.

²¹³ See Article 2(f) and (g) of the eu-LISA 2018 Regulation for which: ‘a high level of data protection, in accordance with Union data protection law, including specific provisions for each large-scale IT system’ and ‘an appropriate level of data and physical security, in accordance with the applicable rules, including specific provisions for each large-scale IT system’.

²¹⁴ See the Council of the EU, 14212/09, Brussels, 9 October 2009 (23.10), p. 14.

²¹⁵ Articles 54 and 55 of the IO Regulations.

²¹⁶ See the C-270/12, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*, for which only ‘precisely delineated’ powers can be delegated to an agency.

²¹⁷ Article 54(3), first and third paragraphs, of the IO Regulations.

²¹⁸ The design and its evolution are adopted by the Management Board following the favorable opinion of the European Commission. The European Commission started issuing its opinion on the interoperability components in autumn 2020.

²¹⁹ Article 54(3), fourth paragraph, of the IO Regulations and Articles 28(5) and (7), 37(4), 38(3), 39(5), and 43(5) of the IO Regulations, as well as Article 78(10) of Regulation (EU) 2019/817 and Article 74(10) of Regulation (EU) 2019/818.

²²⁰ Notably, Articles 72(7) of Regulation (EU) 2019/817 and 68(7) of Regulation (EU) 2019/818 set forth that the European Commission shall inform the European Parliament and the Council of the results of the tests carried out for the ESP, the sBMS, the CIR, the MID, the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum data quality standards, and the CRRS pursuant to paragraphs 1(b), 2(b), 3(b), 4(b), 5(b) and 6(b) of Article 72 of the IO Regulations.

²²¹ Article 54(3), fifth paragraph, of the IO Regulations.

called interoperability components²²² – namely, the ESP²²³, the sBMS²²⁴, the CIR²²⁵ and the MID²²⁶ – and the CRRS²²⁷ that, although formally established by the European Commission through an implementing decision, are tested and validated by eu-LISA. Specifically, the agency is in charge of conducting tests on the algorithms used, for instance, by the MID, which

²²² Notably, the entry into operations of the interoperability components the date from which the majority of the IO Regulations will become applicable. According to Article 79 of Regulation (EU) 2019/817 and Article 75 of Regulation (EU) 2019/818, only the provisions Articles 6, 12, 17, 25, 38, 42, 54, 56, 57, 70, 71, 73, 74, 75, 77 and 78(1) applied since the 11 June 2019. The other ones, instead, are subjected to the adoption of the implementing act of the European Commission establishing the entry into operations of each relevant component. Also, in the case of Eurodac, the IO Regulations are even more “open” since they establish that: ‘This Regulation shall apply in relation to Eurodac from the date the recast of Regulation (EU) No 603/2013 becomes applicable’ – see Article 79(5) of Regulation (EU) 2019/817 and Article 75(9) of Regulation (EU) 2019/818.

²²³ Article 72 of Regulation (EU) 2019/817 and Article 68 of Regulation (EU) 2019/818 specify that the European Commission determines the start operations of the ESP in the thirty days following the adoption of an implementing act and after: the adoption of the implementing measures referred to in Articles 8(2), 9(7), and 43(5) of the IO Regulations; eu-LISA has declared the successful completion of a comprehensive test of the ESP, which it has conducted in cooperation with the Member States authorities and the Union agencies that may use the ESP, and eu-LISA has validated the technical and legal arrangements to collect and transmit the data concerning the ESP-user profiles referred to in Article 8(1) of the IO Regulations and has notified them to the European Commission. Further safeguards have been inserted for the querying of the Interpol’s databases in order not to delay the entry operations of the ESP in the lack of an agreement between the EU and the Interpol.

²²⁴ Article 72(2) of Regulation (EU) 2019/817 and Article 68(2) of Regulation (EU) 2019/818 set forth that the European Commission must determine the date of the entry into operations of the sBMS in thirty days from the adoption of an implementing act, after: the secondary legislation referred to in Articles 13(5) and 43(5) of the IO Regulations have been adopted; eu-LISA has declared the successful completion of a comprehensive test of the sBMS, which it has conducted in cooperation with the Member States authorities; eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Article 13 of the IO Regulations and has notified them to the European Commission, and eu-LISA has declared the successful completion of the test referred to in paragraph 5(b) of Article 72 of Regulation (EU) 2019/817 and Article 68(5)(b) of Regulation (EU) 2019/818 – i.e., the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum data quality standards, which it has conducted in cooperation with the Member States authorities.

²²⁵ The entry into operations of the CIR, instead, is regulated by Article 72(3) of Regulation (EU) 2019/817 and 68(3) of Regulation (EU) 2019/818 for which the European Commission establishes it in thirty days from the adoption of an implementing act, when: the secondary legislation referred to in Articles 43(5) of the IO Regulations, Article 78(10) of Regulation (EU) 2019/817 and Article 74(1) of Regulation (EU) 2019/818 have been adopted; eu-LISA has declared the successful completion of a comprehensive test of the CIR, which it has conducted in cooperation with the Member States authorities; eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Article 18 of the IO Regulations and has notified them to the European Commission, and eu-LISA has declared the successful completion of the test referred to in paragraph 5(b) of Article 72 of Regulation (EU) 2019/817 and 5(b) of Article 68 of Regulation (EU) 2019/818.

²²⁶ The implementing act launching the entry into operation of the MID in the thirty days afterwards must be adopted once: the secondary legislation referred to in Articles 28(5) and (7), 32(5), 33(6), 43(5) and 49(6) of the IO Regulations have been adopted; eu-LISA has declared the successful completion of a comprehensive test of the MID, which it has conducted in cooperation with the Member States authorities and the ETIAS Central Unit; eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Article 34 of the IO Regulations and has notified them to the European Commission; the ETIAS Central Unit has notified the Commission in accordance with Article 71(3) of Regulation (EU) 2019/817 and Article 67(3) of Regulation (EU) 2019/818, and eu-LISA has declared the successful completion of the tests of the ESP, the sBMS, the CIR, and the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum data quality standards.

²²⁷ The CRRS will enter into operations in thirty days as maximum from the adoption of an implementing act following the same paths: the secondary legislation referred to in Articles 39(5) and 43(5) have been adopted; eu-LISA has declared the successful completion of a comprehensive test of the CRRS, which it has conducted in cooperation with the Member States authorities, and eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Article 39 and has notified them to the European Commission.

requires in-depth scrutiny of the quality of the data used to improve the predictive mechanism that is implemented to process data *ex novo*²²⁸. Once the interoperability components have entered into operation eu-LISA will be responsible for the ‘technical management of the central infrastructure of the interoperability components, including their maintenance and technological developments’ which include the relevant communication infrastructure²²⁹. The IO Regulations finally elucidate that eu-LISA has no access to personal data processed through the ESP, the sBMS, the CIR or the MID, without prejudice to Article 62²³⁰. The latter, regulates access to data related to the ESP, the CIR, and the MID, limiting it to the purposes of reporting and statistics.

Together with the Member States, eu-LISA is required to ensure that ‘the best available technology is used, subject to a cost-benefit analysis’²³¹. Article 55(1) of the IO Regulations specifies:

‘Technical management of the interoperability components shall consist of all the tasks and technical solutions necessary to keep the interoperability components functioning and providing uninterrupted services to the Member States and to the Union agencies 24 hours a day, 7 days a week in accordance with this Regulation. It shall include the maintenance work and technical developments necessary to ensure that the components function at a satisfactory level of technical quality, in particular as regards the response time for interrogation of the central infrastructures in accordance with the technical specifications’²³².

The availability of the service must be accompanied by a ‘satisfactory level of quality’ which includes the quickest response time when interrogating the central infrastructure. The necessity of a rapid response was stressed by, and caused concern among, the Member States during the design and developing phases as interoperability will be a key tool for individual checks at the borders – which includes the provision of a new instrument for screening irregular migrants and asylum seekers at the external borders – and a major source of information for the prevention, detection, and investigation of criminal offences²³³. A prompt response is therefore vital in avoiding clogging the external border check points, tracking criminals, preventing potential threats, and efficiently managing mixed flows of third country nationals without unlawfully restricting their rights and freedoms. Thus:

‘All interoperability components shall be developed and managed in such a way as to ensure fast, seamless, efficient and controlled access, full, uninterrupted availability of the components and of the data stored in the MID, the shared BMS and the CIR, and a response

²²⁸ Article 54(3) of the IO Regulations. During the functioning, the agency will keep on managing the realisation of the controls by virtue of Article 55(3) of the IO Regulations.

²²⁹ Article 55(1) of the IO Regulations.

²³⁰ Article 54(3), second paragraph, of the IO Regulations.

²³¹ Article 55(1) of the IO Regulations.

²³² Article 55(1), second paragraph, of the IO Regulations.

²³³ See further Article 22 of the IO Regulations.

time in line with the operational needs of the Member States' authorities and Union agencies'²³⁴.

eu-LISA is also required to 'develop and maintain a mechanism and procedures for carrying out quality checks on the data stored in the sBMS and the CIR'²³⁵ for which purpose the European Commission will adopt an implementing act to establish the date from which the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum data quality standards are to be implemented as laid down in the act of secondary legislation of Article 37(4) of the IO Regulations and after a successful testing has been completed²³⁶. In this respect, eu-LISA is regarded as a key player as far as biometric data is concerned²³⁷ and a roadmap to support Member States in inserting high quality data into the EU information systems was presented in February 2020²³⁸. Indeed, another task related to the principles on the protection of personal data consists of improving the level of accuracy of the data stored in the systems by virtue of the International Organisation for Standardisation's (ISO) standards. eu-LISA's competence in the field of data quality means that it seeks to insert automated data quality checks so as to detect in an automated manner that data that does not comply with predefined quality standards. Along the same line, eu-LISA is competent in adopting common standards of data quality. In the long-term, the possibility to extract quality reports shall be implemented through a common repository containing only anonymised data for reporting and statistics purposes²³⁹. The EDPS welcomed the provision of enhancing data quality parameters and checks, however it opposed the idea of creating a new system storing anonymised data for statistics and, specifically, the possibility that the European Commission, eu-LISA, or the other agencies could have access to it²⁴⁰. Although data accuracy was not covered in the 2011 Regulation, the first activity report states that eu-LISA was expressly in charge of advising Member States on inaccurate data found in the systems 'for transferring or making available to the authorities of third countries data recorded in the system, in cases where the agency is specifically authorised to do so'²⁴¹. eu-LISA has recently received an express

²³⁴ Article 55(1) of the IO Regulations, last paragraph.

²³⁵ Article 37 of the IO Regulations.

²³⁶ See Article 72(5) of Regulation (EU) 2019/817 and Article 68(5) of Regulation 2019/818.

²³⁷ Council of the EU, *Horizontal overview of the biometric data quality and format standards to ensure compatibility of different IT systems in the context of interoperability*, 5924/20, Brussels, 20 February 2020, p. 6: 'eu-LISA provided broad support to the Commission during the preparation of the implementing acts covering biometric data quality. In parallel, the Agency closely supported the Member States on issues related to biometric data quality through its Advisory Groups and by providing the relevant tools. In the context of the implementation of interoperability, this support should be further extended'.

²³⁸ "L'agence européenne pour la gestion opérationnelle des systèmes d'information planche sur la standardisation des données", *Bulletin Quotidien Europe*, No 12851, 11.12.2021.

²³⁹ See Chapter V.

²⁴⁰ See the Council of the EU, 13188/17, Brussels, 13 October 2017, p 11.

²⁴¹ Council of the EU, 6401/13, Brussels, 28 February 2013, p. 13.

empowerment to ensure the quality of the data processed within large-scale IT systems²⁴². Moreover, eu-LISA will ensure the security of the IT infrastructure, of the components – including their maintenance and technological improvements –, and of the relevant communication infrastructure²⁴³. For this purpose, eu-LISA was delegated the task of adopting a security plan, a continuity plan for its activities, and a restoration plan in case of disaster to safeguard the security, integrity and confidentiality of the data²⁴⁴, and has to compensate individuals and any State that suffered any damage as a result of its acts²⁴⁵. eu-LISA's staff is also required to keep professional secrecy, or other equivalent duties of confidentiality as far as the interoperability components are concerned, including after leaving the office or employment with eu-LISA or after the termination of their activities²⁴⁶. Last but not least, eu-LISA provides training on the technical use of the interoperability components²⁴⁷.

As the EDPS has highlighted, the role of eu-LISA in the management of IT systems and the interoperability components implies a series of responsibilities that fall within the definition of a 'data controller' more than a 'data processor'²⁴⁸. Recalling its comment on the SIS:

‘The EDPS understands that due to the growing complexity of the EU large-scale IT systems, eu-LISA may possess specialised knowledge and expertise which may not be available in the Commission services. Nevertheless, the sub-delegation of powers by the Commission to a Union agency raises a number of questions, including about legal competence and allocation of responsibility’²⁴⁹.

²⁴² See Article 12 of eu-LISA 2018 Regulation.

²⁴³ Article 55(1) of the IO Regulations.

²⁴⁴ Articles 42 and 43 of the IO Regulations. See further *infra*.

²⁴⁵ Article 46(1)(b), of the IO Regulations.

²⁴⁶ Article 55(2), first paragraph, of the IO Regulations.

²⁴⁷ Article 55(4) of the IO Regulations.

²⁴⁸ See the Opinion of the EDPS No. 4/2018 on *the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, Brussels, 18.04.2018, pp. 24-25. Similarly, in the *EDPS Formal comments on the draft Commission Implementing Decisions on: 1. the minimum data quality standards and technical specifications for biometric data in the Schengen Information System (SIS) in the field of border checks and return 2. the minimum data quality standards and technical specifications for biometric data in the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters*, Brussels, 26.08.2020, p. 4:

‘[...] the Technical Specifications and SIS Interface Control Document would have direct impact on the means and methods of processing of personal data in SIS of a large number of data subjects, both at central and at national level. Hence, even if the sub-delegation by the Commission to eu-LISA is presumed to be lawful, it still leaves open the question who will bear the responsibility if the implementation of the binding SIS Interface Control Document by Member States or by Europol, Eurojust, etc. leads to risks for the protection of personal data’.

²⁴⁹ Similarly, in the Formal comments of the EDPS on *the draft Commission Implementing Decisions on: 1. the minimum data quality standards and technical specifications for biometric data in the Schengen Information System (SIS) in the field of border checks and return 2. the minimum data quality standards and technical specifications for biometric data in the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters*, Brussels, 26.08.2020, p. 3.

In the EDPS Opinion No. 3/2017, it was pointed out that both ETIAS Central Unit and eu-LISA should have been established as joint controllers²⁵⁰, as eu-LISA also held responsibilities while undertaking its tasks of, for example, developing the system. For this reason, eu-LISA should have been labelled as responsible for the ‘purpose and means’ of the data processing activities conducted within such a system. On the occasion of the drafting of the ECRIS-TCN Regulation, the EDPS proposed to nominate eu-LISA as joint controller together with the national authorities as, among its development tasks, it was in charge of defining the physical architecture, including technical specifications, and of managing in an adequate form the design and the development phases in the Program Management Board²⁵¹. According to the EDPS, ‘[...] where an actor independently defines purposes or means of the data processing it should be considered controller rather than processor’²⁵².

This would at least imply that the burden of the proof with regard to the respect of data protection principles relied on eu-LISA, and not the individual²⁵³. Yet, Article 41 of the IO Regulations confirms that eu-LISA is the data processor of the data processing activities performed in the sBMS, the CIR, and the MID by virtue of Article 12(1) of the EUDPR²⁵⁴. In reality, it is not clear how far eu-LISA will influence the design and the execution of the decisional proceedings flowing from the interoperability architecture. eu-LISA’s “technical” responsibility has crucial impacts on the decision-making procedure, for example, in the frame of Article 21 of the IO Regulations²⁵⁵, though the agency intervenes only indirectly, and it is not a real protagonist regarding the manual verification procedure. Among its tasks is the automated establishment of the white links²⁵⁶ because of which the individual may well suffer important limitations to the exercise of their rights to be informed, access, rectify, suppress, and limit the processing of personal data. The possibility that an automated decision-making process is undertaken by a third party – i.e., the data processor – that is delegated the competence to take decisions further complicates the allocation of responsibilities between data controllers and processors. According to the GDPR, this requires the establishment of certain contractual

²⁵⁰ Opinion of the EDPS No. 3/2017 on the Proposal for a European Travel Information and Authorisation System (ETIAS), Brussels, 6.03.2017.

²⁵¹ Opinion of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011, Brussels, 2.03.2021.

²⁵² *Ibid.*, para. 40.

²⁵³ Article 4(2) EUDPR.

²⁵⁴ Article 41 of the IO Regulations.

²⁵⁵ See Chapter V.

²⁵⁶ *Ibidem*.

terms with processors²⁵⁷ in order to make the use of sub-contractors lawful. Recalling the EDPS's words:

'The EDPS notes that the Proposal does not address the issue of subcontracting a part of the Commission tasks to another organisation or entity (such as a private company). Nevertheless, subcontracting is commonly used by the Commission in the management and development both of the system and the communication infrastructure. While the subcontracting does not in itself run contrary to data protection requirements, important safeguards should be put in place to ensure that the applicability of Regulation 45/2001, including the data protection supervision by the EDPS remains entirely unaffected by the subcontracting of activities. Furthermore, additional safeguards of a more technical nature should also be adopted. In this regard, the EDPS suggests that similar legal safeguards as envisaged in the SIS II legal instruments should be provided in the framework of the revision of the EUODAC Regulation, specifying that even when the Commission entrusts the management of the system to another authority, this shall "not adversely affect any effective control mechanism under Community law, whether of the Court of Justice, the Court of Auditors or the European Data Protection Supervisor (Article 15 par. 7, SIS II Decision and Regulation). The provisions are even more precise in Article 47 of the SIS II Regulation, which stipulates: "Where the Commission delegates its responsibilities (...) to another body or bodies (...) it shall ensure that the European Data Protection Supervisor has the right and is able to fully exercise his tasks, including carrying out on-the-spot checks and to exercise any other powers conferred on him by Article 47 of Regulation (EC) No 45/2001". The above-mentioned provisions provide for a necessary clarity in terms of the consequences of subcontracting a part of the Commission tasks to other authorities. The EDPS therefore suggests that provisions aiming at the same effect be added to the text of the Commission's Proposal'²⁵⁸.

Although, this possibility was not inserted under Article 4 of the recast Eurodac Regulation of 2013²⁵⁹, it becomes of paramount importance in the interoperability discourse. In this context, eu-LISA's decisions are never issued to the individual, however, the agency supports the administrative procedure which may impact the individual's rights regarding the protection of personal data. It is true that eu-LISA activity may not 'directly' concern the individual in the light of the TFEU²⁶⁰, which would exclude any chance of taking the agency before the CJEU. Yet, the powerlessness of the individual in addressing certain agencies' decisions or implementations is not a new phenomenon. As Prof. Esteve García points out:

'[...] doubts remain about certain acts of the agencies which cannot be formally or clearly considered as "acts intended to produce legal effects vis-à-vis third parties", because

²⁵⁷ Article 28 GDPR.

²⁵⁸ Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], COM(2008) 825, Brussels, 20.02.2009.

²⁵⁹ See the discussions on the Eurodac in the Council of the EU, *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person]* (recast), 8474/09, Brussels, 14 April 2009, p. 3.

²⁶⁰ Article 263, fourth paragraph, TFEU.

they constitute intermediate, advisory or internal acts, but which de facto come to have great relevance or influence on the final decision taken by a given European institution, or by the Member States themselves²⁶¹.

Notably, the fact that eu-LISA is not the controller of the data processing activities prevents it from accessing the logs – i.e. ‘[...] rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality’²⁶² – of Articles 10, 16, 24 and 36 of the IO Regulations and excludes the placing of any ‘other-monitoring’ mechanism over them. Logs are important when retracing the chain of operations carried out by each national authority or staff member²⁶³ according to Articles 20, 21 and 22 of the IO Regulations. Even if the access to, and exchange of, data under its activity is recorded at the central level, the keeping of logs on the data processing operations²⁶⁴ is a shared task between eu-LISA, the other Union bodies that have access to the interoperability components, and the Member States. In the case of the EES²⁶⁵, for example, the agency keeps: the date and time of the processing activity, the type of data transmitted, the type of data used for interrogation, and the name of the authority entering or retrieving the data. In addition, it is up to the Member State to keep records of the staff duly authorised to input or retrieve the data. In this sense, Member States prefer to monitor compliance with the Regulation through the logs by implementing “self-monitoring” procedures rather than empowering the agency – or the European Commission – to do so²⁶⁶.

Interoperability's purposes	Article 20	Article 21	Article 22
Logs held by eu-LISA according to Article 24 of the IO Regulations	- the Member State or Union agency launching the query;	- the Member State or Union agency querying the CIR;	- the Member State or Union agency querying the CIR;
	- the purpose of access for the user querying via the CIR;		

²⁶¹ Francina Esteve García, “El Control Judicial de las Agencias del Espacio de Libertad, Seguridad y Justicia”, in Cristina Blasi Casagran and Mariona Illamola Dausá, *El control de las agencias del Espacio de Libertad, Seguridad y Justicia*, Madrid, Marcial Pons, 2016, pp. 81-104, p. 88 (our own translation).

²⁶² European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 64.

²⁶³ Articles 10, 16, 24, and 36 of the IO Regulations for the ESP, the sBMS, the CIR, and the MID.

²⁶⁴ See Article 30 of the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union*, 6928/13, Brussels, 28 February 2003.

²⁶⁵ See Article 46 of the EES Regulation.

²⁶⁶ See Article 31 of the Council of the EU, 6928/13, Brussels, 28 February 2013.

	- the date and time of the query;	- the date and time of the query;	- the date and time of the query;
	- the type of data used to launch the query;	- the data used to launch the query;	- the data used to launch the query;
	- the results of the query.	- the results of the query.	- the results of the query.

Figure 1 Logs held by eu-LISA for Articles 20, 21, and 22 of the IO Regulations – Source: Own elaboration.

3. The cooperation of eu-LISA domestically and internationally

3.1. The exchange of personal data with EU institutions, bodies, and offices

The intra-institutional exchange of information, and particularly personal data, is sealed by working agreements that eu-LISA can adopt with Union institutions, bodies, and offices by taking into account the opinion of the European Commission²⁶⁷. eu-LISA has concluded inter-institutional agreements with the following bodies: European Anti-Fraud Office (OLAF)²⁶⁸; the EUAA²⁶⁹; the European Union Agency for Cybersecurity (ENISA)²⁷⁰; Eurojust²⁷¹; Europol²⁷²; and the FRA²⁷³. Additional amendments to expand eu-LISA's competences in statistics would have been required with regard to the regulation of each system. As for statistics, Member States suggested that eu-LISA should have reported statistics to the European Commission for the Schengen Evaluation mechanism (SCH-EVAL)²⁷⁴, to the EBCG Agency for the vulnerability assessment, and to other agency for justified purposes²⁷⁵.

²⁶⁷ See Article 41 of eu-LISA 2018 Regulation.

²⁶⁸ Council of the EU, *Accession of the European Agency for operational management of large-scale IT systems in the area of freedom, security and justice to the Interinstitutional Agreement of 25 May 1999 concerning internal investigations by the European Anti-Fraud Office (OLAF)*, 14805/12, Brussels, 8 October 2012.

²⁶⁹ See the Working arrangement between the EUAA and eu-LISA of 4 November 2014, available at www.eulisa.europa.eu (all the arrangements and MoUs are available here). The two agencies have also signed a Cooperation Plan 2020-2022 – see the “eu-LISA and EASO Sign a Three-Year Cooperation Plan”, *Press Release*, 15 November 2020, available at the same webpage.

²⁷⁰ See the MoU (working arrangement) between ENISA and eu-LISA of 10 January 2018.

²⁷¹ See the MoU between Eurojust and eu-LISA of 9 September 2017. Note that the Memorandum allows for the exchange of information but not operational data relating to an identified or identifiable person under Article 3(2). On 11 October 2021, eu-LISA and Eurojust signed a Cooperation Plan 2021-2023 moving forward the digitalisation of the justice domain, especially in view of the implementation of the e-CODEX by eu-LISA – see the “eu-LISA and Eurojust Consolidate Their Cooperation in the Justice Domain”, *Press Release*, 11 October 2021, available at www.eulisa.europa.eu.

²⁷² See the MoU between Europol and eu-LISA of 22 March 2016.

²⁷³ See the Working arrangement between the FRA and eu-LISA of 6 July 2016.

²⁷⁴ Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen, *OJ L* 295, 6.11.2013, pp. 27-37.

²⁷⁵ See Finland suggestions in the Council of the EU, 11884/17, Brussels, 13 September 2017, p. 15. To be noted that eu-LISA's participation in the SCH-EVAL is contemplated by the Proposal for a Council Regulation on the

The intra-agency cooperation with the EBCG Agency also covers the fields of researching, testing, and developing IT systems, among which the study on biometrics stands out. eu-LISA collaborates with the EBCG Agency²⁷⁶, CEPOL²⁷⁷, and the Member States directly for the purposes of reporting, publishing, monitoring, and issuing information, as well the organisation of specific trainings²⁷⁸. For example, the EBCG Agency-eu-LISA working arrangement²⁷⁹ is focused on the use of large-scale IT systems in the frame of the EBCG Agency's operational activities and is directed through annual operational planning agreed among the parties. Specifically, eu-LISA is authorised to provide the EBCG Agency with statistical and anonymous data stemming from the management of large-scale IT systems to enrich the situational and risk analyses the EBCG Agency is called to generate. In turn, eu-LISA can develop and tailor services for the EBCG Agency on the basis of its empirical experience. Besides, the two agencies also cooperate regarding ICT projects and services as was experimented with the establishment of the ETIAS Central Unit, as well as for research and development activities with a particular focus on technology. Any processing of personal data is regulated by the current EUDPR, and a specific commitment to the confidentiality of information has been agreed.

eu-LISA is expected to actively contribute to the EUAA's capacity building cooperation, under which framework a joint activity on the use of Big Data technology²⁸⁰ for forecasting and monitoring long-term migration trends, migration categories/indicators, and timeframes will be developed. Specifically, eu-LISA must ensure that the CRRS architecture corresponds to the end-user's needs: 'The agencies will exchange information on analysis relevant developments in requesting access to large-scale EU IT systems for analysis and reporting'²⁸¹. The EUAA-eu-LISA working arrangement²⁸² was signed on 4 November 2014 and relates to the following

establishment and operation of an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing Regulation (EU) No 1053/2013, COM(2021) 278 final, Brussels, 2.6.2021, that was validated by the Member States on the 27 April 2022 according to "Les États membres de l'UE valident la réforme du mécanisme d'évaluation Schengen", *Bulletin Quotidien Europe*, No. 12940, 28.4.2022. The Proposal is expected to expand the scope of the SCH-EVAL to all large-scale IT systems and to the interoperability framework too so that the EDPS suggested to widen its policy fields too – see the Opinion of the EDPS No. 10/2021 on the *Proposal for a Council Regulation on the establishment and operation of an evaluation and monitoring mechanism to verify the application of the Schengen acquis*, Brussels, 27.07.2021, p. 6.

²⁷⁶ See the Working arrangement between the EBCG Agency and eu-LISA of 31 January 2014.

²⁷⁷ See the Working arrangement between CEPOL and eu-LISA, the date is not specified.

²⁷⁸ See Articles 1(4) and 6 of 2011 eu-LISA Regulation.

²⁷⁹ Working arrangement between the EBCG Agency and eu-LISA of 31 January 2014.

²⁸⁰ Big Data relies not only on the increasing ability of technology to support the collection and storage of large amounts of data, but also on its ability to analyse, understand and take advantage of the full value of data (in particular using analytics applications). See for example, the Opinion of the EDPS No. 7/2015, *Meeting the challenges of big data: A call for transparency, user control, data protection by design and accountability*, Brussels, 19.11.2015.

²⁸¹ EUAA-EBCG Agency cooperation plan of 18 July 2019, p. 6.

²⁸² Working arrangement between the EUAA and eu-LISA of 4 November 2014.

fields of cooperation: exchange of information, statistics, analyses and reports; ICT-related matters; training provided to Member States; operational support and expert assistance; strategic and administrative matters, and other areas identified as mutually important. The exchange of information, statistics, analyses, and reports shall take place in compliance with the data privacy and information security provisions that support both agencies' activities. The cooperation on ICT matters covers the know-how, expertise, best practices, lessons learned and advice in technical, operational and IT security matters as well as business continuity in ICT. The regime on the protection of personal data refers to the ECDPR as far as data is processed by EU institutions and bodies, and to Regulation (EC) 1049/2001²⁸³ regarding access to public documents. From the Annual Cooperation Plan of 2017, it is understandable that the two agencies cooperate for in establishment of identification and registration matters, the implementation of the forthcoming Eurodac, as well as the better use of the DubliNet that must be fed with high quality data, customised statistics and reports, and the use of the ESP in the frame of the IO Regulations²⁸⁴. Thus, eu-LISA plays a significant role in enhancing the operational and technical reinforcement of Member States' capacities in cases of serious challenges regarding migration as is the case regarding 'large inward migratory flows':

‘Such reinforcement is provided in hotspot areas through the deployment of relevant teams composed of experts from relevant European Union Agencies. The Agencies may plan and carry out pilot projects encompassing inter alia standardisation of equipment for migration management support teams (MMSTs), if relevant’²⁸⁵.

The 2020-2022 Cooperation Plan foresees the implementation of innovative solutions based on the use of AI and machine-learning for ‘technical and practical tools used in the asylum procedure’²⁸⁶. It is not clear, however, which guarantees are going to be made on the processing of personal data as the reports limit themselves to saying that: ‘The agencies will exchange the lessons learnt and best practices in the area of personal data protection’.

Last but not least, in the EES Proposal, the question of training staff involved in the running of the system was especially emphasised since it is the Member States' direct responsibility to ensure that the systems work properly²⁸⁷. It shall be noted that among these trainings, eu-LISA

²⁸³ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, *OJ L* 145, 31.5.2001, pp. 43-48.

²⁸⁴ See further Chapter V.

²⁸⁵ See the Cooperation Plan 2020-2022 between eu-LISA and the EUAA.

²⁸⁶ *Ibid.*, p. 3.

²⁸⁷ See the Opinion of the European Economic and Social Committee on the ‘Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System’ (COM(2016) 196 final — 2016/0105 (COD)) and on the ‘Proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC)

is in charge of the SIRENE staff as well as that of SCH-EVAL. Europol and Eurojust are allowed to participate in the Management Board as observers for the aspects related to the systems' police purposes²⁸⁸, while the EBCG Agency can attend those meetings that relate to its mandate²⁸⁹ or to the ETIAS. Europol and Eurojust also attend eu-LISA's Advisory Group²⁹⁰.

3.2. Any transfer of data to third countries and international organisations?

In the preparatory works on the 2011 Regulation, it was clarified that in no case would the operational management have enabled the agency to exchange data or share information and knowledge²⁹¹. Only those countries that have entered into agreements with the Union on who, through their association with the implementation, application, and development of the Schengen *acquis* and with Dublin- and Eurodac-related measures, can benefit from cooperation with eu-LISA²⁹². The possibility that eu-LISA could share information not only within the EU but also with third countries through working agreements was debated during the negotiations of the 2018 Proposal²⁹³. The 2018 Regulation delegates the mandate to cooperate with international organisations and other relevant entities²⁹⁴ by means of working arrangements to eu-LISA. These arrangements must be concluded with the authorisation of the Management Board and after having received approval from the European Commission. Unfortunately, these working arrangements have not been subjected to any data protection requirement, which may become crucial in light of the forthcoming EU-Interpol agreement, which is expected to require eu-LISA's support for its implementation²⁹⁵.

No 767/2008 and Regulation (EU) No 1077/2011' (COM(2016) 194 final — 2016/0106 (COD)), *OJ C* 487, 28.12.2016, pp. 66-69.

²⁸⁸ See Article 22 of eu-LISA 2018 Regulation.

²⁸⁹ 2019 EBCG Agency Regulation.

²⁹⁰ See Article 19(3) of 2011 eu-LISA Regulation.

²⁹¹ *Ibidem*.

²⁹² Article 42(1) of eu-LISA 2018 Regulation.

²⁹³ See recital (34) of the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011 - General approach*, 14807/17, Brussels, 24 November 2017.

²⁹⁴ Article 43 of eu-LISA 2018 Regulation.

²⁹⁵ See Chapter VI.

CHAPTER V

THE INTEROPERABILITY OF LARGE-SCALE IT SYSTEMS IN THE AREA OF FREEDOM, SECURITY AND JUSTICE: CONTEXT, CONTENT AND PURPOSES

Regulations (EU) 817 and 818 of 2019¹ establish a framework for the interoperability of six large-scale IT systems currently in existence or that are soon to be implemented within the AFSJ. These systems were analysed in depth in Chapter III and are²: the SIS; the VIS; the EES; the ETIAS; the Eurodac, and the ECRIS-TCN. The sister Regulations³ aim at interconnecting these six large-scale IT systems under the auspices of a new IT infrastructure that supports their functioning.

Regulations (EU) 817 and 818 of 2019 have been criticised⁴ for being overly complex and excessive technical, which would hinder a comprehensive understanding of their scope. Interoperability seems to contribute to the layering of EU regulations on large-scale IT systems, adding nothing but opacity and a challenge to the protection of individuals' rights⁵. Indeed, interoperability poses many challenges to the protection of the individuals' human and

¹ To be noted that the interoperability established by Regulations (EU) 2019/817 and 2019/818 shall be differentiated from other system-to-system forms of interconnection – e.g., the automated querying to the VIS performed by the EES – that are also labelled as ‘interoperability’ as we explained in Chapter III.

² For the time being, decentralised databases like PNR, API, European Police Records Index System (APRIs), and the Prüm Decision have been excluded from the interoperability architecture, though in the impact assessment realised for the interoperability Proposals were taken into account – see the Commission Staff Working Document impact assessment, Accompanying the document Proposal for a Regulation of the European Council on establishing a framework for interoperability between eu information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 and Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between eu information systems (police and judicial cooperation, asylum and migration), SWD(2017) 0473 final, Strasbourg, 12.12.2017. These systems need to be centralised before being interconnected to the interoperability architecture. Although the European Commission is already moving ahead with this project – see the Roadmap, Border and law enforcement - advance air passenger information (API) - revised rules, and the attached Inception Impact Assessment, available at www.ec.europa.eu, as well as the Proposal for a “Prüm II” Regulation – it is still early to extend our research to them. Preliminary remarks on interoperability for PJCCM purposes have been made by Francesca Galli, “Interoperable Law Enforcement: Cooperation Challenges in the EU Area of Freedom, Security and Justice”, *EUI Working Papers*, No. 15, 2019, pp. 1-20, and Athina Giannakoula, Dafni Lima, and Maria Kaiafa-Gbandi, *Combating Crime in the Digital Age: a Critical Review of EU Information Systems in the Area of Freedom, Security and Justice in the Post-Interoperability Era*, Leiden/Boston, Brill, 2020.

³ As renamed by the Opinion of the EDPS No. 4/2018 on *the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, Brussels, 18.04.2018, p. 9.

⁴ Among others, see Evelien Brouwer, 2020, *op. cit.*, p. 90: ‘As underlined by the EDPS in the aforementioned Opinion 4/2018, the IO Regulations only add another layer to the complexity of practices and laws of existing data systems. This complexity of rules triggers further questions on accountability and liability with regard to incorrect or unlawful data processing’.

⁵ See the Opinion of the EDPS No. 4/2018 on *the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, Brussels, 18.04.2018, pp. 9-10, and in the literature, for instance: Hartmut Aden, “Interoperability Between EU Policing and Migration Databases: Risks for Privacy”, *European Public Law*, Vol. 26, No. 1, 2020, pp. 93-108, and Florin Coman-Kund, “Europol’s International Exchanges of Data and Interoperability of AFSJ Databases”, *European Public Law*, Vol. 26, No. 1, 2020, pp. 181-204.

fundamental rights⁶ and, above all, the data protection principles as interpreted by international and supranational jurisprudence⁷. Given that these principles are being put under strain, the lawfulness of interoperability has been questioned by scholars⁸ in light of the limitation principle and/or the proportionality principle⁹. However, other authors believe such a close inspection is not useful, highlighting how the co-legislators have been extremely cautious regarding the data protection package, both in its design and implementation phases¹⁰.

This Chapter explores the true colours of “freedom, security and justice legal interoperability” beyond the mere interconnection of the six underlying large-scale IT systems so as to shed light on its impact on the EU data protection *acquis*, both in terms of the exercise of the Union’s competence based on Article 16(2) TFEU and in respect of the fundamental rights to the protection of personal data set forth in Article 8 of the CFREU, from a legal perspective. Here, we start with a brief historical background on the interoperability package to highlight the context¹¹ surrounding the adoption of Regulations (UE) 2019/817 and 2019/818. Opting for a systemic interpretation of the correlated legislative reforms in the AFSJ – i.e., the enhanced empowerment of agencies operating in the freedom and security areas regarding the

⁶ Confront the FRA, *Fundamental rights and the interoperability of EU information systems: borders and security*, Vienna, 2017, recalling: the right to an effective remedy (Article 47) or the prohibition of torture and inhuman or degrading treatment or punishment (Article 4); liberty and security of person (Article 6); integrity of the person (Article 3); the right to asylum (Article 18) and prohibition of collective expulsion (Article 19); rights of the child (Article 24), and equality before the law (Articles 20) of the CFREU.

⁷ See Pika Šarf, “Automating Freedom, Security and Justice: Interoperability of AFSJ Databases as a Move Towards the Indiscriminate Mass Surveillance of Third-Country Nationals”, in Aleš Završnik and Vasja Badalič, *Automating Crime Prevention, Surveillance, and Military Operations*, Switzerland, Springer, 2021, pp. 85-108.

⁸ Deirdre Curtin and Filipe Brito Bastos, 2020, *loc. cit.*, and Hartmut Aden, *loc. cit.*

⁹ See, for example, Niovi Vavoula, “Interoperability of EU Information Systems in a ‘Panopticon’ Union: A Leap Towards Maximised Use of Third-Country Nationals’ Data or Step Backwards in the Protection of Fundamental Rights?”, in Valsamis Mitsilegas and Niovi Vavoula, *Surveillance and Privacy in the Digital Age: European Transatlantic and Global Perspectives*, London, Hart Publishing, 2021, pp. 159-195, and the Meijers Committee standing committee of experts on international immigration, refugee and criminal law, *CM1802 Comments on the Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)*, Leiden, 12 December 2017, available at www.statewatch.org. Also, the Opinion of the Article 29 DPWP on *Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration*, Brussels, 11.04.2018, has been especially critic, for instance, because of the storage of biometric data in a unique centralised “database”.

¹⁰ Elisabeth Hoffberger-Pippan, “The Interoperability of EU Information Systems and Fundamental Rights concerns”, *Spanish Yearbook of International Law*, No. 23, 2019, pp. 426-250, p. 428, according to whom: ‘For the time being, however, the Regulation can be summarised as a positive step forward in order to face current challenges adequately, while at the same time making sure that fundamental rights are sufficiently protected’.

¹¹ See C-431/11, *United Kingdom of Great Britain and Northern Ireland v Council of the European Union*, 26 September 2013, EU:C:2013:589, para. 36. Note that Paula García Andrade, 2018, *op. cit.*, p. 183, warns that: ‘[...] this element should, in my view, be taken with caution since it might lead to attention turning to the objectives of other measures related to the act rather than on the specific objectives of the act in question’. In previous Chapters we advanced that the development of the interoperability architecture is physically bound to the development of large-scale IT systems, and we will here appreciate that its objectives and content almost retrace the one set forth in the systems’ regulations. In these terms, the ‘context’ of the IO Regulations is of the outmost importance not only to understand its roots, but also to anticipate its possible development in the future.

management of personal data processed by “multi-purpose” large-scale IT systems¹² – we should appreciate that interoperability is but the tip of the iceberg of a wider project that aims to put in place an EU model for the management of information for freedom, security and justice purposes. The objectives and content of the sister Regulations are analysed to assess how much weight is given to data protection in such a framework in view of the fact that Article 16(2) TFEU is taken, for the first time ever in the field of IT, as the correct legal basis regarding freedom, security and justice. The extent of the legal frameworks underpinning both Regulations (EU) 2019/817 and 2019/818 may be misleading if one considers that the EU policies on borders, visas, asylum, migration, police cooperation, and judicial cooperation in the criminal field are put on an equal footing with the EU competence on the protection of personal data and the free movement of such data. It is therefore unclear from this legal framework whether, and in what terms, interoperability contributes to the underlying EU competences, including Article 16(2) TFEU. Besides, such overreaching frameworks risk going beyond the EU’s competences contained under the AFSJ, and our analysis will extend accordingly.

1. The interoperability of large-scale IT systems: Historical background

Generally speaking, the word “interoperability” is used in reference of the ‘ability of systems to exchange and make use of information in a straightforward and useful way; this is enhanced by the use of standards in communication and data format’¹³ or, more broadly, as ‘[t]he ability of entities in a network to connect with each other and carry out their functions; for example, the ability of some proprietary software to operate properly as a part of the Internet by communicating with several technologies’¹⁴. Therefore, the concept of interoperability

¹² See Chapters III and IV respectively.

¹³ “Interoperability”, in Andrew Butterfield, Gerard Ekembe Ngondi, and Anne Kerr, *Dictionary of Computer Science*, Oxford, Oxford University Press, 2016, available at www.oxfordreference.com. Other definitions given, for example, by the International Electrotechnical Commission, are presented by Jörg Hoffmann and Begoña Gonzalez Otero, “Demystifying the Role of Data Interoperability in the Access and Sharing Debate”, *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, Vol. 11, No. 3, 2020, pp. 252-273, p. 25, who analyse the interoperability among data – personal and not – in the frame of the Digital Strategy of the EU available at digital-strategy.ec.europa.eu.

¹⁴ See “Interoperability”, in Darrel Ince, *A Dictionary of the Internet*, Oxford, Oxford University Press, 2019, www.oxfordreference.com.

contemplates an intrinsic technical substrate¹⁵ the “neutrality”¹⁶ of which must be modelled on the policy area within which it is implemented. While relying on the ISO, Prof. Santusuosso and Prof. Malerba outline four distinct concepts of interoperability:

- ‘technical interoperability’, regarding signals between devices;
- ‘syntactic interoperability’, that is, the ability of diverse systems to communicate with each other and exchange data;
- ‘semantic interoperability’¹⁷, namely, the ability to interpret and use data and pieces of information in a significant way that is useful to the end user, and
- ‘organisational interoperability’, acting on a political stage which requires the linkage of different administrative procedures and institutional bodies¹⁸.

Interoperability is intended to resolve “communication issues” among different cultures while embracing ‘[...] the idea of making systems (of any kind, not only those belonging to information and communication technology (ICT)) that are characterised by diverse dimensions and structures fit with one another and communicate, without losing their peculiarities’¹⁹. Prof.

¹⁵ The Working Document of the Article 29 DPWP on *E-Government*, Brussels, 8.05.2003, early defined interoperability as the ‘setting up and promoting the on-line supply of administrative procedures’ among which it contemplated: the institution of a unique entry point to online administrative services; the establishment of unique identifiers, or the implementation of interconnected public databases. In this regard, consult the Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (Text with EEA relevance) PE/41/2018/REV/2, *OJ L* 295, 21.11.2018, pp. 1-38, and the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, *OJ L* 257, 28.8.2014, pp. 73-114. The Article 29 DPWP well highlighted that a balance was needed between interconnection – and the supposed improvement of services of the administration – and the protection of users’ personal data – p. 10.

¹⁶ Opinion of the EDPS on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability, COM(2005) 490 final, *OJ C* 116, 17.05.2006, p. 8, para. 17.

¹⁷ Dag Wiese Schartum, “Sharing Information between Government Agencies: Some Legal Challenges Associated with Semantic Interoperability”, in Simone van der Hof and Marga M. Groothuis, *Innovating Government. Normative, Policy and Technological Dimensions of Modern Government*, The Hague, Springer, 2011, pp. 347-362, p. 361, brings the example of the Norwegian legislation to highlight how the use of ‘computer-friendly legislation’ entailing the use of the same wording for almost identical legal concepts regulated under different legislations may not be compatible with the necessary flexibility requested to interpret and modify the law over time.

¹⁸ ISO/IEC 2382-1, Information technology — Vocabulary — Part 1: Fundamental terms, 1993. Amedeo Santusuosso and Alessandra Malerba, “Legal Interoperability as a Comprehensive Concept in Transnational Law”, *Law, Innovation and Technology*, Vol. 6 No. 51, 2014, pp. 51-73, pp. 52-53, recall that the word ‘interoperability’ has been abundantly used in the frame of military operation. See, for example: Andrew Clapham, “Human Rights in Armed Conflict: Metaphors, Maxims, and the Move to Interoperability”, *Human Rights & International Legal Discourse*, Vol. 12, No. 1, 2018, pp. 9-22; Colonel Kirby Abbott, “A brief overview of legal interoperability challenges for NATO arising from the interrelationship between IHL and IHRL in light of the European Convention on Human Rights”, *International Review of the Red Cross*, No. 96, Vol. 893, 2014, pp. 107-137; John R. Den, “Maintaining transatlantic strategic, operational and tactical interoperability in an era of austerity”, *International Affairs (Royal Institute of International Affairs 1944-)*, Vol. 90, No. 3, 2014, pp. 583-600.

¹⁹ Jörg Hoffmann and Begoña Gonzalez Otero, *op. cit.*, p. 256, find that ‘[...] one of its primary benefits is that interoperability can preserve key elements of alternative technical solutions and thus innovation and competition while ensuring that systems to work together’.

Beydogan, instead, talks about ‘convergence [...] as a multi-level compatibility problem, specifically at the network, service, content and terminal equipment levels’²⁰ for which purpose ‘[...] the use of common standards and protocols, or the use of a conversion function to map between different services would be required’²¹. According to the above-mentioned authors, the EU represents the ‘most significant examples of the usefulness of the concept of cultural (and political) interoperability [...] with the ambition to shape a unique system of governance and politics based on a single market [...]’²². Working within different legal systems (those of the Member States) and different languages (at least, twenty-three official languages), the EU would integrate one of the three facets²³ of the so-called ‘legal interoperability’ that constitutes a fifth and final interpretation to consider²⁴. In this regard, the recent definition proposed by the OECD is notable:

“‘privacy interoperability’ can thus be understood operationally as the ability of different privacy and data protection regimes, or legal frameworks, to work together at multiple levels through policy and practical arrangements and thereby bridge any differences in approaches and systems of privacy and personal data protection to facilitate transborder flows of personal data’²⁵.

However, Prof. Palfrey and Prof. Gasser clearly explain that any theory on interoperability leaves ‘most of the specificities of how to bring interop about to be determined on a case-by-case basis [...] The price to be paid for striving for a universal principle at the level of theory is that such a theory is full of nuances when it comes to application in practice’²⁶. Therefore, any interoperability framework must be contextualised in order to envision its real range²⁷.

As Prof. De Hert and Prof. Gutwirth²⁸ highlight, the continental concept of interoperability is inscribed within the “e-initiatives” family²⁹ and has been used in a wide range of public law

²⁰ Turgut Aythan Beydogan, "Interoperability-Centric Problems: New Challenges and Legal Solutions", *International Journal of Law and Information Technology*, Vol. 18, No. 4, 2010, pp. 301-331, p. 304.

²¹ *Ibidem*.

²² *Ibid.*, p. 56.

²³ *Ibid.*, p. 59, refer also to the possibility that interoperability is applied within the same legal system (or state) using the same language – likes it happens for example, in the US federation –, or among different legal systems using the same language – which happens among the common law countries.

²⁴ Anna Zharova, "Influence of the Principle of Interoperability on Legal Regulation", *International Journal of Law and Management*, Vol. 57, No. 6, 2015, pp. 562-572, p. 565, referring to the specific case of Russian Federation.

²⁵ OECD Going Digital Toolkit, *Interoperability of privacy and data protection frameworks*, Paris, 2021, p. 11.

²⁶ John Palfrey and Urs Gasser, *op. cit.*, pp. 17-18.

²⁷ This allows us to distance ourselves, for example, from studies carried out in the health sector where interoperability has been the subject of study for over forty years according to Oscar Aleixo Costa Rocha, *Adapting a System-Theoretic Hazard Analysis Method for Interoperability of Information Systems in Health Care*, LL.M. Dissertation in Computer Science, University of Victoria, 2022, p. 7.

²⁸ Paul De Hert and Serge Gutwirth, “Interoperability of police databases within the EU: An accountable political choice?”, *International Review of Law, Computers & Technology*, Vol. 20, No. 1-2, 2006, pp. 21-35, p. 23.

²⁹ While referring to Regulations (EU) 2019/817 and 2019/818, the study for the LIBE Committee of Mirja Gutheil, Quentin Liger, James Eager, Yemi Ovosu, and Daniel Bogdanovic, *Interoperability of Justice and Home Affairs Systems*, PE 604.947, Brussels, 2018, p. 11, weirdly affirms that: ‘The roots of the definition can be clearly traced

domains³⁰ following the presentation of the pan-European e-Government initiative³¹. In these terms, interoperability is presented as an old project that dates back to the pre-Lisbon era as far as the AFSJ is concerned. In the authors' words:

'Certainly, the rising of the issue of interoperability has been triggered by the launching and development of 'e-initiatives' (such as eGovernment and eHealth), which demand smooth and easy communication between all the concerned actors (services, business, customers, citizens, etc.). It is also clear that the question of interoperability has been raised in respect of many policy fields as identified by a survey carried out by Kubicek and Cimander: state and society (eParticipation, eDemocracy); social affairs (health pensions, social security); education, science and research; economy and labour; infrastructure; taxes and customs; and police, security and justice'³².

Early discussions on the matter raised issues on whether interoperability is in fact a long-term project or whether it has been recently revisited by the co-legislators. In the following paragraphs we will briefly retrace the steps taken by the co-legislators in 2000s leading up to

back to the field of e-Government, but the application requires much greater clarity on how the concept of interoperability – in particular, the notions of legal, semantic, operational and technical interoperability – has been applied to the creation and design of the solutions'. In the case of e-Government for judicial cooperation see the Council of Europe Recommendation of the Committee of Ministers on *the interoperability of information systems in the justice sector*, REC(2003)14, Strasbourg, 9 September 2003, and Francesco Contini and Giovan Francesco Lanzara, *The Circulation of Agency in E-Justice. Interoperability and Infrastructures for European Transborder Judicial Proceedings*, Dordrecht Heidelberg New York London, Springer, 2014.

³⁰ For example, the eHealth network was established in 2011 to promote the interoperability of national health systems so as to exchange patients' data on e-Prescriptions, Patient Summaries, and electronic health records – see the Commission Implementing Decision 2019/1765 of 22 October 2019 providing the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth, and repealing Implementing Decision 2011/890/EU (notified under document C(2019) 7460) (Text with EEA relevance) C/2019/7460, *OJ L* 270, 24.10.2019, pp. 83-93, commented by the Joint Opinion of the EDPS-EDPB on *eHDSI*, Brussels, 12.07.2019. Also, interoperability was mandated the difficult task of restoring the free movement of individuals within the Schengen area in the aftermath of the COVID-19 pandemic through the so-called Digital Green Certificate for vaccinated, recovered, and tested persons as commented in the Joint Opinion of the EDPB-EDPS No. 04/2021 on *the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate)*, Brussels, 31.03.2021, p. 14. Other fields of application that can be mentioned are: the development of a personal information management systems; the enhancement of contestability and the access to the market in the frame of the Digital Market Act – see "DMA, les seuils de désignation et l'interopérabilité au cœur de l'accord provisoire entre le PE et le Conseil de l'UE", *Bulletin Quotidien Europe*, No. 12919, 26.3.2022 –, and the promotion of common standards for online platforms according to the Digital Service Act – see the Opinion of the EDPS No. 2/2021 on *the Proposal for a Digital Markets Act*, Brussels, 10.02.2021, and the Opinion of the EDPS No. 1/2021 on *the Proposal for a Digital Services Act*, Brussels, 10.02.2021.

³¹ See the Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on the interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC), *OJ L* 144, 30.4.2004, pp. 64-73, and the European Commission Communication, Interoperability for Pan-European e-Government Services, COM(2006) 45 final, Brussels, 13 February 2006. These were replaced by the Interoperability solutions for European public administrations (ISA), *OJ L* 260, 3.10.2009, p. 20, upon which the European Commission approved the European Interoperability Strategy (EIS) and the EIF. On the concept of e-Government see Corien Prins and Wim Voermans, "A Brave New Government?", in Simone van der Hof and Marga M. Groothuis, *op. cit.*, pp. 455-466, p. 451, maintaining that: 'Linking systems requires more than merely connecting ICT. Essential prerequisites in addition to technical interoperability are organizational interoperability, legal interoperability, as well as semantic interoperability'. On the specific sector of eHealth see Kärt Salumaa-Lepik, Tanel Kerikmäe and Nele Nisu, "Data Protection in Estonia", in Elif Kiesow Cortez, *Data Protection Around the World: Privacy Laws in Action*, The Hague, Springer, 2020, pp. 23-58.

³² Paul De Hert and Serge Gutwirth, *op. cit.*, p. 23.

the adoption of the interoperability package in support of the freedom, security and justice policies this Chapter is scrutinising.

1.1. Interoperability in the aftermath of 11-S

The word ‘interoperability’ took root in the European Community’s agenda after 11-S and was first discussed as a means to interconnect existing systems that were collecting data from third country nationals. In the Conclusions of the Council Meeting held in Laeken on 14 and 15 December 2001³³, Member States were invited to strengthen their controls at the external borders and, under pressure from US counter-terrorism policy³⁴, work on a common visa identification system began. It was the Spanish Delegation that, during the VIS negotiations, wondered whether both the SIS and the VIS might be merged³⁵. Later on, after the terrorist attacks of 2004 and 2005, the interconnection of the Eurodac was also envisaged. As a result, the European Commission was formally asked to submit a new proposal in order to exploit the added value of existing and future systems ‘[...] within their respective legal and technical framework’³⁶. In The Hague Programme of March 2005, the European Council requested the Council of the EU:

‘[...] to examine how to maximise the effectiveness and interoperability of EU information systems in tackling illegal immigration and improving border controls as well as the management of these systems on the basis of a communication by the Commission on the interoperability between the Schengen Information System (SIS II), the Visa Information System (VIS) and EURODAC to be released in 2005, taking into account the need to strike the right balance between law enforcement purposes and safeguarding the fundamental rights of individuals’³⁷.

From the early debates, interoperability acquired an added value for EU policies on PJCCM³⁸ since it aimed at ‘[...] linking and merging national databases of law enforcement

³³ Presidency Conclusions European Council meeting in Laeken 14 and 15 December 2001, DOC/01/18, available at www.ec.europa.eu.

³⁴ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Public Law 107–56 — Oct. 26, 2001, available at www.congress.gov.

³⁵ See the Council of the EU, *Note sent by the Spanish delegation sent to the Visa Working Party on Databases of visas*, 15577/01, Brussels, 21 December 2001, p. 4, recalled by Evelien Brouwer, 2008, *op. cit.*, pp. 117-144.

³⁶ See also the Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597 final, Brussels, 24.11.2005, and the Council of the EU, *Note of the Secretariat General of the Council of the European Union on the Declaration on combating terrorism*, 7906/04, Brussels, 9 March 2004, p. 8, in Comments of the EDPS on *the Communication of the Commission on interoperability of European databases*, Brussels, 10.03.2006.

³⁷ The Hague Programme: strengthening freedom, security and justice in the European Union, OJ C 53, 3.3.2005, pp. 1-14.

³⁸ As for PJCCM interoperability was criticised by the EDPS also in view of the Proposal on a Europol Decision – ‘According to Article 10(5) of the proposal, every effort shall be made in order to ensure interoperability with the data processing systems in the Member States and with the systems in use by the Community and Union related bodies. This approach reverses the approach of the Europol Convention (Article 6(2)), which prohibits the linking

containing DNA or fingerprint’ which put interoperability on track with the legislator tendency of granting law enforcement authorities and intelligence services’ access to “migration databases”³⁹. However, legal, political, and technical concerns⁴⁰ prevented the European Commission from presenting a proposal for a Regulation on the interoperability of the SIS, the VIS, and the Eurodac. First of all, the lack of uniform data protection criteria among the Member States – especially as far as the PJCCM areas were concerned – was depicted as ‘an open invitation to discrimination and excessive discretion’ when it came to regulating the processing of personal data in police databases⁴¹. In an underdeveloped IT environment where new technological expedients had not yet been explored – e.g., cloud computing, big data, and machine learning techniques – some technical aspects were also unclear. As the EDPS highlighted⁴², the concept of interoperability proposed by the European Commission was used ‘not only in relation to the common use of large-scale IT systems, but also with regard to possibilities of accessing or exchanging data, or even of merging databases’⁴³. Also, the EDPS noted that the European Commission’s Communication provided for new objectives for large-scale IT systems that called for a new assessment of their impact on the protection of personal data⁴⁴. Biometrics were proposed as the ‘primary key’ – i.e., a unique number referring to an item in order to gather the data – in breach of the principle of data quality. In these terms, the issue of biometrics served to catalyse the joining of different databases into an interconnected

to other automated processing systems’ in the Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision establishing the European Police Office (Europol), COM(2006) 817 final, Brussels, 27.10.2007 –, and in the frame of the e-Justice reform that aimed at facilitating the public’s access to justice and communication among judicial authorities and achieve substantial economies of scale at European level – see the Opinion of the EDPS on the Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee towards a European e-Justice Strategy, OJ C 276/8, Brussels, 6.6.2009, paras. 23 and 24:

‘The EDPS recommends that the interconnection and interoperability of systems should duly take into account the purpose limitation principle and be built around data protection standards (privacy by design). Any form of interaction between different systems should be thoroughly documented. Interoperability should never lead to a situation where an authority, not entitled to access or use certain data, can obtain this access via another information system. The EDPS wants to stress again that inter- operability should not by itself justify circumventing the purpose limitation principle’.

³⁹ Niovi Vavoula, 2020, *op. cit.*, p. 148.

⁴⁰ Peter Hobbing, *Briefing paper: An analysis of the commission communication (COM (2005) 597 final of 24.11.2005) on improved effectiveness, enhanced interoperability and synergies among European databases in the area of justice and home affairs*, IP/C/LIBE/FWC/2005-08, Brussels, 14.02.2006, urging consistency among existing databases legal frameworks and democratic oversight on the European Parliament behalf.

⁴¹ Paul De Hert, *What are the risks and what guarantees need to be put in place in view of interoperability of police databases?*, IP/C/LIBE/FWC/2005-25, Brussels, 1.02.2006, p. 3.

⁴² Comments of the EDPS on the Communication of the Commission on interoperability of European databases, Brussels, 10.03.2006.

⁴³ *Ibid.*, p. 2.

⁴⁴ *Ibid.*, p. 3.

network that was expected to promote the establishment of increasingly decentralised systems.

In the EDPS' words:

‘This aggregation of databases also increases the risk of "function creep" when the interlinking of two databases designed for two distinct purposes will provide a third one for which they have not been built, a result which is in a clear contradiction of the purpose limitation principle’⁴⁵.

Moreover, the exchange of information through the new interoperability architecture⁴⁶ would enable direct access to information held by other Member States which would ‘[...] automatically mean that an increased number of persons will have access to a database and therefore encompasses a growing risk of misuse’⁴⁷. All in all, the EDPS asked the European Commission for ‘a more consistent analysis on data protection, including privacy-enhancing technologies, to improve both effectiveness and data protection’⁴⁸. A last daunting factor highlighted by the European Parliament was the existence of an inter-pillars structure that prevented the EU from adopting a common EU policy on personal data, crosscutting the whole AFSJ. According to Prof. Kindt and Prof. Müller:

‘[...] whatever the interpretation of the concept, it cannot be denied that in the Third Pillar policy area of Justice and Home Affairs interoperability potentially has a much more intruding effect and can touch fundamental rights, and privacy and data protection issues’⁴⁹.

⁴⁵ *Ibid.*, p. 4.

⁴⁶ Andrew Butterfield, Gerard Ekembe Ngondi, and Anne Kerr, “architecture”, in Andrew Butterfield, Gerard Ekembe Ngondi, and Anne Kerr, *A Dictionary of Computer Science*, 2016, available at www.oxfordreference.com:

‘The specification of a (digital) computer system at a somewhat general level, including description from the programming (user) viewpoint of the instruction set and user interface, memory organization and addressing, I/O operation and control, etc. [...] In the context of engineering and hardware design, the term architecture is used to describe the nature, configuration, and interconnection of the major logic organs of a computer (and is thus closer to the general meaning of the word). These devices would normally include the memory and its components, the control unit and the hardware components designed to implement the control strategy, the structure, range, and capability of the ALU, and the interconnection of the input/output—such as whether star or bus connected—and the nature and capabilities of any channel controllers. A detailed block diagram or schematic of the actual (as distinct from the virtual) machine would normally form part of, or even be central to, such a description’.

⁴⁷ Opinion of the EDPS on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability, COM(2005) 490 final, OJ C 116, 17.05.2006, p. 8, para. 35, and Paul De Hert, *What are the risks and what guarantees need to be put in place in view of interoperability of police databases?*, IP/C/LIBE/FWC/2005-25, Brussels, 1.02.2006, p. 9:

‘The idea of interoperability should be implemented with care and respect for the plurality of the good. In our social democratic state, citizens have to deal with government for a number of reasons. It would be disrespectful of the ideas behind data protection to see government as a whole that may use 'its' information, taken from whatever governmental database, at random. Limited interoperability needs to be the rule; exceptions to this rule (immediate or unmediated interoperability) should be carefully assessed in the light of the rules and the rationale between the existing (separated) domains. The goal should be an intelligent police, not an all-knowing police’.

⁴⁸ Comments of the EDPS on the Communication of the Commission on interoperability of European databases, Brussels, 10.05.2006, p. 4.

⁴⁹ Els Kindt and Lorenz Müller, *D3.10: Biometrics in identity management*, Future of Identity in the Information Society, Brussels/The Hague, 2007, pp. 1-130.

The interconnection of police databases with ‘other systems’ was highlighted, since the uncontrolled access of law enforcement authorities to ‘migration’ databases could have led to abuses, especially because the roles of intelligence and police authorities were increasingly overlapping and becoming confused⁵⁰. Thus, interoperability suddenly became a ‘[...] highly sensitive political issue as it has the potential of striking citizens right at the heart of their social, political and cultural wellbeing’⁵¹. In sum, the implementation of interoperability was not governed by the availability of information, but rather represented a revolutionary change in the administration of public policies for which a wider debate was needed, with, and within, civil society.

1.2. The adoption of the interoperability package

The interoperability project was resumed in 2016 following the communitarisation of the PJCCM area and, consequently, the possibility of inserting a horizontal legal basis conferring on the EU the competence to regulate the protection of personal data and the free movement of such data emerged⁵². While submitting the interoperability Proposals, the European Commission was counting on the Member States’ support⁵³ as their positions had been felt out with the presentation of the strategy on Stronger and Smarter Information Systems for Borders and Security in Brussels on 6 April 2016⁵⁴. On that occasion, the European Commission stressed the need to improve the efficiency of existing IT systems and to furnish the EU with new databases to fill in information gaps:

‘[...] the architecture of data management for borders and security is fragmented, as information is stored separately in unconnected systems. This leads to blind spots. As a consequence, the various information systems at EU level are currently not interoperable — that is, able to exchange data and share information so that authorities and competent officials have the information they need, when and where they need it. Interoperability of EU-level information systems can significantly contribute to eliminating the current blind

⁵⁰ Gianfranco Marullo, *loc. cit.*

⁵¹ Els Kindt and Lorenz Müller, *loc. cit.*, and Paul De Hert and Serge Gutwirth, *loc. cit.*

⁵² See Chapter I.

⁵³ See the Council of the UE, *European Council meeting (17 and 18 December 2015) – Conclusions*, EUCO 28/15, Brussels, 18 December 2015, and the Council of the UE, *Conclusions of the European Council meeting*, EUCO 34/16, Brussels, 15 December 2016, p. 3, according to which: ‘The co-legislators should agree by June 2017 on the Entry/Exit System and by the end of 2017 on a European Travel Information and Authorisation System to ensure that visa-exempt travelers are screened systematically. It also calls for continued delivery on the interoperability of information systems and data bases’.

⁵⁴ Communication from the Commission to the European Parliament and the Council, Stronger and Smarter Information Systems for Borders and Security, COM(2016) 205 final, Brussels, the 6.04.2016, p. 14 ff. See also the Statement of the President of the European Commission Jean-Claude Juncker on the State of the Union of 14 September 2016, available at www.ec.europa.eu: ‘We will defend our borders, as well, with strict controls, adopted by the end of the year, on everyone crossing them. Every time someone enters or exits the EU, there will be a record of when, where and why’.

spots where persons, including those possibly involved in terrorist activities, can be recorded in different, unconnected databases under different aliases⁵⁵.

Among other points, the European Commission stressed that data regarding long-term visas was not stored in any centralised databases and it was impossible to be certain that visa-exempt travellers were leaving the Schengen area upon the expiration of their visa. Moreover, even if law enforcement authorities were granted the right to access third country nationals' data stored in the existing systems, the existing silo-architecture slowed down the process and, therefore, impeded a prompt response in the face of terrorist and serious criminal threats. The European Commission found that much of the data was incomplete and stored in an inaccurate manner, while others represented overlaps as the same categories of data were kept separately in different systems. Needless to say: the combination of the 2015 humanitarian crisis together with long term terrorist threats helped the European Commission to gain the support of civil society⁵⁶ as well as the European Parliament. According to the latter, the European Commission should '[...] address information gaps and move towards interoperability, as well as proposals for compulsory information sharing at EU level, accompanied by necessary data protection safeguards⁵⁷.

The interoperability package is rooted in the mandate the Member States conferred on the co-legislators to reform EU information tools under The Netherlands Presidency⁵⁸. Following the Netherlands Presidency, three Presidencies had been especially relevant regarding the negotiations on the interoperability package: the Bulgarian, which obtained the mandate for starting the legislative process; the Austrian Presidency, that led during the trialogue and reached a first agreement on the "sister Proposals" and, finally, the Romanian Presidency, that had to deal with a huge number of technical aspects and achieved the final accordance. Under the Netherlands' leadership, the HLEG on information systems and interoperability was established⁵⁹ as a political group chaired by DG HOME and gathering representatives from: the Member States and the Schengen Associated Countries, freedom, security and justice agencies

⁵⁵ Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)*, 15729/17, Brussels, 14 December 2017, p. 1.

⁵⁶ Report on Europeans' attitudes towards security' analyses the results of the Special Eurobarometer public opinion survey (464b) regarding citizens' overall awareness, experiences and perceptions of security, available at www.europa.eu.

⁵⁷ Council of the EU, *Resolution of the European Parliament on the strategic priorities for the Commission's work programme for 2017*, 2016/2773 (RSP), Brussels, 6 July 2016, point 29.

⁵⁸ See the Council of the EU, *Roadmap of 6 June 2016 to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area* —, 9368/1/16 REV 1, Brussels, 6 June 2016.

⁵⁹ Commission Decision of 17 June 2016 setting up the high-level expert group on information systems and interoperability C/2016/3780, *OJ C* 257, Brussels, 15.7.2016, pp. 3-6.

– namely, eu-LISA, the EBCG Agency, the FRA, the EUAA, and Europol –, the Counter-Terrorism Coordinator (CTC), the EDPS and two observers – i.e., the Council Secretariat and one representative of the LIBE Committee⁶⁰. Despite the European Ombudsman's decision⁶¹, the HLEG never published⁶² the names of its members, including the Member States' authorities, and of the observers in the Register of expert groups⁶³, which reveals transparency gaps attributable to the EU institutions. The HLEG gathered in Brussels five times and adopted its opinions, recommendations, or reports by consensus⁶⁴. On 20 June 2016, a Roadmap to enhance information exchange and information management, including interoperability solutions in the JHA Area, was agreed in order to lay out the steps to be followed to create the EU smart borders strategy for enhancing security within the Schengen area⁶⁵. Its implementation was monitored by the Standing Committee on Operational Cooperation on Internal Security (COSI) on a yearly basis and flowed into a final report which was adopted in May 2017⁶⁶. From all of this, it can be understood that the European Commission was shifting

⁶⁰ Its mandate focused on: the improvement of implementation and use by Member States of existing systems, including the possibility to make them more effective, process-oriented, and user-friendly; the development of new systems to address identified gaps in the present information system landscape, and the development of an interoperability vision for the next decade that reconciles process requirements with data protection safeguards. See, among others, the Council of the EU, *Information Technology (IT) measures related to border management* a) Systematic checks of external borders b) Entry/Exit System (EES) c) Evolution of the Schengen Information System (SIS) d) EU Travel Information and Authorisation System (ETIAS) e) High-Level Expert Group on Information Systems and Interoperability = Progress report, 12661/16, Brussels, 3 October 2016, p. 8.

⁶¹ European Ombudsman, *Decision in case 1276/2018/FP on the European Commission's alleged failure to disclose the names of the national authorities participating in the High-Level Expert Group on Information System and Interoperability*, Strasbourg, 20.03.2019.

⁶² See the Register of Commission Expert Groups and Other Similar Entities available at www.ec.europa.eu. From it, several subgroups specifically dedicated to the EU systems and interoperability were set up.

⁶³ Article 11(2) of the Commission Decision of 17 June 2016 setting up the high-level expert group on information systems and interoperability C/2016/3780, *OJ C* 257, 15.7.2016, pp. 3-6.

⁶⁴ *Ibid.*, Article 5(6).

⁶⁵ Council of the EU, *Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area*, 7711/16, Brussels, 12 April 2016. The roadmap was endorsed to the European Commission by the Justice and Home Affairs Council. Development on the implementation of the Roadmap were debated on the 8 November 2016 – Council of the EU, *Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area: - State of play of its implementation*, 13554/1/16 REV 1, Brussels, 8 November 2016 – and on the 1 and 8 June 2017 – Council of the EU, *Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area: - State of play of its implementation (second implementation report)*, 8433/17, Brussels, 11 May 2017. On the 7 December 2017, the Roadmap was updated as suggested by the HLEG on information systems and interoperability – Council of the EU, *Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area: - Update following Council Conclusions on interoperability*, 14750/17, Brussels, 24 November 2017, and Council of the EU, *Conclusions of the Council of the European Union on the way forward to improve information exchange and ensure the interoperability of EU information systems*, 10151/17, Brussels, 14 June 2017. Afterward, a third report was published in Council of the EU, *Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area: - State of play of its implementation (third implementation report)*, 7931/1/18 REV 1, Brussels, 22 June 2016.

⁶⁶ Council of the EU, *High-level expert group on information systems and interoperability. Final report*, Ares(2017) 2412067, Brussels, 11.05.2017.

the management of the EU external borders from a “digital” to a “smart” architecture characterised by a strong security component made up of enhanced, dislocated controls at, beyond, and within the Schengen area⁶⁷.

Under the Malta Presidency of 2017, the EU Council reaffirmed its full support to the interoperability project⁶⁸ and exhorted the European Commission to adopt a legislative proposal. Therefore, a Eurobarometer survey was launched to discover if EU citizens felt safe within the free movement area⁶⁹, while stakeholders were involved through the organisation of several seminars. Unfortunately, the European Commission’s consultation enjoyed very little feedback from the public⁷⁰: the European Commission received only eighteen replies according to the briefing on the EU Legislation process on interoperability between EU border and security information systems prepared by Luyten and Sofija Voronova in June 2019⁷¹. Moreover, from an in-depth analysis, we noted that only one of the documents sent out directly referred to the purposes of the interoperability package – i.e., the exchange of information between law enforcement authorities in the context of the fight against crime and terrorism⁷² – which undermines the reliability of the survey *vis-à-vis* the sister Proposals. All in all, the European Commission believed that it had sufficient support⁷³ to present its Proposals, and did so in December 2017⁷⁴.

The negotiations around the interoperability package were incredibly quick⁷⁵, not only because of the consent expressed by the Member States’ delegations during the preparatory

⁶⁷ Interestingly, the debate on the construction of anti-migrants’ wall has been fouled by the ongoing negotiations on the Pact on Asylum and Migration proposed by the European Commission on 23 September 2020, published at the European Commission’s webpage at www.ec.europa.eu. See the “Manfred Weber estime que le budget européen doit pouvoir financer des clôtures anti-migrants”, *Bulletin Quotidien Europe*, No. 12821, 28.10.2021.

⁶⁸ See the Council of the EU, 10151/17, Brussels, 14 June 2017.

⁶⁹ See the Document of the Director General Migration and Home Affairs, *Special Eurobarometer 464b: Europeans’ towards security*, TNS opinion and political Wave EB87.4, Brussels, 2017, p. 40 ff.

⁷⁰ Katharina Eisele, “Interoperability between EU information systems for security, border and migration management”, *Initial Appraisal of a European Commission Impact Assessment*, PE 615.649, 2018.

⁷¹ See the position of the European Parliament, *Interoperability between EU information systems for security, border and migration management*, PE 628.267, 06.2019, p. 7. The outcome of the Eurobarometer is available at www.ec.europa.eu.

⁷² The application was worded as follows: ‘To combat crime and terrorism, should the [national] police and other law enforcement authorities exchange information with the authorities of the other EU countries on a case-by-case basis or always?’. Possible answers were: a) on a case-by-case basis; b) always and c) in all cases.

⁷³ The European Commission met with the European Parliament and the Council on 17 November 2017.

⁷⁴ Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JAI, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, COM(2017) 0793 final, Brussels, 13.12.2017, and Proposal for a Regulation of the European Parliament and of the Council on the establishment of a framework for the interoperability of EU information systems (police and judicial cooperation, asylum and migration), COM(2017) 0794 final, Brussels, 13.12.2017.

⁷⁵ The SIS, VIS, and Eurodac Supervision Coordination Groups complained about the rushed discussions on such a complex process – see the Council of the EU, *Opinion on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, 10484/18, Brussels, 27 June 2018.

work⁷⁶, but also because of the approaching European Parliament election of 2019⁷⁷. Indeed, a major change in the makeup of European Parliament might have slowed down the entire process if case negotiations had been reopened, as happened with the revised VIS Proposal, political agreement upon which within the Council was reached only in December 2020⁷⁸. It should be noted that the presentation of two new sister Proposals regarding the interoperability consequential amendments⁷⁹ already required the revision of the mandate given to the Council of the EU and the nomination of new rapporteurs, Jeroen Lenaers and Nuno Melo, by representatives of the LIBE Committee, as well as other relevant experts within it. The rapporteurs were responsible for monitoring the negotiations on the interoperability package: the former for the management of external borders and migration issues; the latter for PJCCM and asylum cooperation. If the interoperability package was adopted after the 2019 Parliament elections, two new rapporteurs would have been nominated. Moreover, the alliance established among the three main political groups that had been supporting the interoperability package from the very beginning – namely, the European People’s Party, the Progressive Alliance of Socialists and Democrats, and the Alliance of Liberals and Democrats for Europe – might have changed. The Alliance of Liberals and Democrats for Europe was the party most involved in the reforms, while the European People’s Party and the Progressive Alliance of Socialists and Democrats showed some concerns regarding the protection of fundamental rights and,

⁷⁶ Note that the Member States’ Parliament could have submitted their opinions on the principle of subsidiarity by the 16 April 2018, yet there was no opposition in these terms – see the European Parliament, *Interoperability between EU border and security information systems*, Brussels, 2019.

⁷⁷ See the Report of the Council of the EU, *The future of EU migration and asylum policy — Outcome of discussions*, 14364/19, Brussels, 22 November 2019. Differently, the Eurodac whose recast was deadlocked under the Romanian Presidency is still kept as a hostage together with the asylum package although it has been revised with the new Pact on Asylum and Migration – see Chapter III.

⁷⁸ See Chapter III.

⁷⁹ See the Council of the EU, *Amended proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) and amending [Regulation (EU) 2018/XX [the Eurodac Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of law enforcement], Regulation (EU) 2018/XX [the ECRIS-TCN Regulation] and Regulation (EU) 2018/XX [the eu-LISA Regulation]*, 10190/18, Brussels, 15 June 2018, and the Council of the EU, *Amended proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399, Regulation (EU) 2017/2226, Regulation (EU) 2018/XX [the ETIAS Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of border checks] and Regulation (EU) 2018/XX [the eu-LISA Regulation]*, 10178/18, Brussels, 15 June 2018. Consequential amendments were added later one since some of the systems – namely, ETIAS, ECRIS-TCN, SIS, and Eurodac – as well as eu-LISA’s mandate were still under negotiations at the time of the first interoperability Proposals, with the sole exception of the EES. The revised VIS Proposal, instead, was about to be proposed – see the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA, COM(2018) 302 final, Brussels, 16.5.2018, analysed in Chapter III. In any case, no substantial change was brought with the submission of the new Proposals.

specifically, the right to the protection of personal data. The coalitions established before the 2019 elections did in fact shift as a result of the elections: the Progressive Alliance of Socialists and Democrats and the European People's Party Groups lost influence and allied with one another, while the Renew Europe Group received the majority of the votes. In sum, the European Commission might have envisaged having to cope with less political support but, it could not have fully predicted the outcome of the European Parliament elections.

During the negotiations, several informal meetings were held among the European Commission, the European Parliament, and the Council of the EU in so-called trialogue formations⁸⁰. Trialogues expressed the compromise sought by the Council of the EU before the enhanced power conferred on the European Parliament in the co-decision procedure after the Lisbon Treaty entered into force. According to Prof. Costa and Prof. Brack:

‘This process of ‘pre-cooking’ the texts, inspired by the conciliation committee of the co-decision, allowed an increasing number of them to vote straight after the first reading; a decrease in the number of rejected proposals as well as a decrease in the number of amendments proposed by the EP and the Council’⁸¹.

Trialogues have become a consolidated⁸² fast-track tool for use in the ordinary legislative procedure – especially in view of the sensitive topics debated within DG HOME as, regrettably, this procedure is performed behind closed doors – and they are finally formalised in a joint declaration on practical arrangements for co-decision⁸³. As far as the interoperability package

⁸⁰ Interoperability trialogues were held on 24 October 2018, 15 and 17 November 2018, 13 December 2018 and on 5 February 2019 according to the European Parliament, *Interoperability between EU border and security information systems*, Brussels, 2019, p. 10.

⁸¹ See Costa Olivier and Brack Nathalie, *How the EU really works*, New York, Routledge, 2019, p. 238. The author explains how trialogue works in practice in the box available at p. 240. According to them, the trialogue conformation demands for the delegation of a mandate, and negotiations only begins when the work group and parliamentary committee in charge of the file have adopted their amendments and have given the negotiators a sort of mandate. Meetings are usually held four to six times. The European Parliament has the major number of delegations (twenty members) composed of: the rapporteur, the chair of the parliamentary committee, the shadow rapporteurs or coordinators, the administrators of the groups, and the administrators of the general secretariat. The Council is represented by ten people: the President of the Committee of the Permanent Representatives of the Governments of the Member States to the European Union (COREPER) or the working group; one or two representatives of the Presidency; three or four administrators of the unit in charge of the case, and a representative of the Legal Service. The European Commission is represented by a dozen or so of people: the Director General; the Director or Head of Unit concerned; the administrators of the unit dealing with the case; the administrators of the units responsible for relations with the Council and the Parliament, and an agent.

⁸² Trialogue is supported by Article 295 TFEU that encourages the development of inter-institutional procedures on the sidelines of the founding Treaties' procedures.

⁸³ The Joint Declaration on practical modalities for co-decision of 30 June 2007 is part of the Better Regulation Agreement signed on 16 December 2003, that defines what ‘best practice’ consists in and sets targets and commitments of each institutions in the matter – see also the Declaration No 34 on respect for time limits under the co-decision procedure annexed to the Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, *OJ C* 340, 10.11.1997, pp. 1-144. On 9 March 2016, under the Juncker's administration, another Better Regulation Statement was agreed with a special impact on the European Commission, and specifically on: the elaboration of impact assessment, the justification of the principles of proportionality and subsidiarity, the adoption of measures on economic, social and

is concerned, trialogues mainly covered technical content⁸⁴ and pivoted around the CIR that was looked at with suspicion by the European Parliament. Among points, the European Parliament fought to improve the safeguard contained in Article 20 of the IO Regulations and to preserve the cascade mechanism in Article 22⁸⁵. In addition, the European Parliament required the provision of a web portal to enforce the exercise of data protection rights by individuals subjected to the multiple detection procedure, which is now sealed in Article 49 of the IO Regulations. A final political compromise was found under the Romanian Presidency during the first reading⁸⁶ on 5 February 2019 as this was supported by a passing vote among the members of the European Parliament on 27 March 2019 – with 511 votes to 123 and 9 abstentions for the borders and visa file, and 510 votes to 130 and 9 abstentions for the law enforcement and migration file⁸⁷ – and by the Council of the EU on 14 May 2019⁸⁸. Regulation (EU) 2019/817 and Regulation (EU) 2019/818 establishing a framework for the interoperability of freedom, security and justice large-scale IT systems were adopted on 20 May 2019, a few days before the latest parliamentary elections⁸⁹, saving precious time and avoiding a re-opening

environmental plans, the consultation with stakeholders etc. – see the Communication from the Commission, Better Regulation: Delivering better results for a stronger Union, COM(2016) 615 final, Brussels, 14.9.2016.

⁸⁴ There are different kind of trialogues: an informal dialogue made up of bilateral meetings between the Parliament and the Council without the Commission; technical preparatory trialogues intended to deal with ‘technical details’; and the ‘political trialogues’ where the final agreement is negotiated – see Costa Olivier and Brack Nathalie, *op. cit.*, p. 238.

⁸⁵ See *infra*.

⁸⁶ Trialogue might take place during the first or the second reading. In case of conciliation, the negotiations are always held in trialogue and the Conciliation Committee validate the final result. However, it shall be recalled that the European Commission can amend its proposal only in the first reading so that it is in this phase when the European Commission remains actively involved. During the second reading, instead, the Council and the European Parliament may reach an agreement on the grounds of the proposed amendments which could seriously distort the original Commission’s proposal – see Costa Olivier and Brack Nathalie, *loc. cit.*

⁸⁷ See the Council of the EU, *Amended proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) and amending [Regulation (EU) 2018/XX [the Eurodac Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of law enforcement], Regulation (EU) 2018/XX [the ECRIS-TCN Regulation] and Regulation (EU) 2018/XX [the eu-LISA Regulation]] - Outcome of the European Parliament’s first reading (Strasbourg, 15 to 18 April 2019)*, 7751/19, Brussels, 25 April 2019.

⁸⁸ Noting that the trialogue give a special leading role to the Presidency of the Council in the negotiations since it might represent the unique hope to adopt the legislative proposal in its mandate – still, Costa Olivier and Brack Nathalie, *loc. cit.*

⁸⁹ Only the United Kingdom abstained from voting Regulation (EU) 2019/818, but its position did not break the consensus among the Member States in view of its withdrawal from the EU – see the Council of the EU, – *Voting result – Regulation of the European Parliament and of the Council establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/... – Adoption of the legislative act 3689th meeting of the Council of the European Union (Agriculture and Fisheries), 14 May 2019*, 9258/19, Brussels, 14 May 2019. Besides, its lack of support was motivated not for the integration procedure but, on the contrary, for its desire to facilitate the access of law enforcement authorities to migrant’s data according to Article 22 of the IO Regulations – i.e., the (no) suppression of the cascade approach as explained *infra* – see its statement in Council of the EU, *Draft Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and*

of the European Commission's Proposals. However, shortly after their publication in the *OJ*, the sister Regulations had to be amended following the reform of the Visa Code, which suggested that the race against technology had just begun.

2. The range of the interoperability Regulations

The IO Regulations consider interoperability as a semantic reform consisting of the ability of information systems to exchange data and to enable the sharing of information⁹⁰. Yet, the now famous statement of the EDPS recalls:

‘Interoperability is not only or primarily a technical choice but rather a political choice liable to have profound legal and societal consequences that cannot be hidden behind allegedly technical changes. The decision of the EU legislator to make large-scale IT systems interoperable would not only permanently and profoundly affect their structure and their way of operating, but would also change the way legal principles have been interpreted in this area so far and would as such mark a ‘point of no return’⁹¹.

The lack of a legal definition of interoperability prevents a straightforward understanding of the range of the IO Regulations *vis-à-vis* freedom, security and justice policies. The IO Regulations are grounded in a composite legal framework, similarly to that of the eu-LISA, with the sole exception being that a reference to Article 16(2) TFEU has been finally inserted following the CJEU's *Opinion 1/15*⁹². Specifically, the legal bases composing Regulation (EU) 2019/817 and Regulation (EU) 2019/818 reflect those underpinning large-scale IT systems and those identifying some of the freedom, security and justice agencies that are granted access to the systems⁹³. As a result, the legal bases regarding law enforcement and those relating to Europol and Eurojust are clear, while those relating to the EBCG Agency and the EUAA are backed up by Articles 77(2)(d) and 78 TFEU respectively. As a result of interoperability, all freedom, security and justice policies will benefit from a unique architecture with the sole exception of judicial cooperation in civil matters⁹⁴. However, and although the Treaty of Lisbon suppressed the interpillar structure, the AFSJ still constitutes a patchwork of dispositions in which the Member States retain elements of their sovereign competences due to the various policies designed to accommodate their needs. By accepting the presence of multiple legal bases, the European Commission undertook a hazardous step before the horizontal subdivision

migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/... (first reading) - Adoption of the legislative act – Statement, 8733/1/19 REV 1 ADD 1, Brussels, 8 May 2019.

⁹⁰ Communication from the Commission to the European Parliament and the Council, COM(2016) 205 final, Brussels, the 6.04.2016.

⁹¹ Opinion of the EDPS No. 4/2018 on *the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, Brussels, 18.04.2018, p. 3.

⁹² See *Opinion 1/15*, and Chapter I.

⁹³ See previous Chapter III.

⁹⁴ Chapter III of Title V TFEU.

of competences between the EU and the Member States⁹⁵ as it sought to avoid absorbing Member States' sovereign prerogatives.

In the following paragraphs we will explore the scope of interoperability by taking into account, first, whether the sister Regulations constitute a development of the Schengen *acquis* or not. Recalling the CJEU jurisprudence on the choice of the correct legal basis, although '[...] the question whether a measure constitutes a development of the Schengen *acquis* is separate from that of the legal basis on which that development must be founded'⁹⁶, variable geometry must be treated '[...] by analogy with what applies in relation to the choice of the legal basis of a Community act'⁹⁷. Turning to the assessment of the content and purposes of the sister Regulations, we will be able to understand how much Article 16(2) TFEU weighs on the IO Regulations⁹⁸, both in quantitative and qualitative terms⁹⁹, *vis-à-vis* the other EU legal bases involved. Recalling Advocate General Mengozzi's *Opinion 1/15*:

'[...] If an examination of the EU measure reveals that it pursues a twofold purpose or that it has a twofold component, and if one of those is identifiable as the main or predominant purpose or component, whereas the other is merely incidental, the act must be based on a single legal basis, namely, that required by the main or predominant purpose or component'¹⁰⁰.

Such analysis 'must rest on objective factors which are amenable to judicial review, including in particular the aim and the content of the act [...]'¹⁰¹.

⁹⁵ Especially as for those provisions that enable Member States to opt for a reinforced cooperation so that Member States can dictate the rhythm of the integration of determined policies – see Costa Olivier and Brack Nathali, *op. cit.*, p. 226.

⁹⁶ See C-482/08, *United Kingdom of Great Britain and Northern Ireland v Council of the European Union*, paras. 64 and 65.

⁹⁷ *Ibid.*, para. 77.

⁹⁸ Which gave positive results, for example, in C-43/12, *European Commission v European Parliament and the Council*, 6 May 2014, EU:C:2014:298, where the CJEU from the analysis on the purposes and content found that Directive 2011/82/EU of the European Parliament and of the Council of 25 October 2011 aimed to improve road safety which is a prime objective of the EU's transport policy under Article 91(1) TFEU.

⁹⁹ This theory is especially important in order to channel the correct proceeding for concluding international treaties – see Article 218 TFEU – and it has gained further attention where the CFSP that is regulated under Title V of the TEU – blurs the line with the external dimension of the police cooperation – Chapter 5 of Title V TFEU. Confront Paula García Andrade, "La base jurídica de la celebración de acuerdos internacionales por parte de la UE: entre la PESC y la dimensión exterior del Espacio de Libertad, Seguridad y Justicia. Comentario a la sentencia del Tribunal de Justicia de 14 de junio de 2016, Asunto C-263/14, Parlamento c. Consejo", *Revista General de Derecho Europeo*, No. 41, 2017, pp. 128-160.

¹⁰⁰ Advocate General Mengozzi, *Opinion 1/15*, para. 61 and the jurisprudence therein recalled C-377/12, *Commission v. Council*, para. 34, and C-130/10, *European Parliament v Council of the European Union*, 19 July 2012, EU:C:2012:472, paras. 42 to 45.

¹⁰¹ See C-77/05, *United Kingdom of Great Britain and Northern Ireland v Council of the European Union*, para. 77.

2.1. Interoperability in-between the Schengen *acquis* and the Area of Freedom, Security and Justice

The rationale underlying the splitting of the IO Regulations goes back to the different degrees of participation by Member States and third countries in freedom, security and justice policies, also known as “variable geometry”¹⁰². The legal frameworks concerning interoperability embrace systems that are a development of the Schengen *acquis* – i.e., the VIS¹⁰³, the EES, and the ETIAS – and others that are not – i.e., the Eurodac¹⁰⁴ and the ECRIS-TCN¹⁰⁵. The SIS falls under the umbrella of interoperability but, unlike from any other system, it is burdened by its controversial nature: on the one hand, the SIS lies at the crossroads between the freedom and security sections; on the other hand, some SIS alerts carry the burden of an ambiguous policy – i.e., the prevention and combat of illegal migration by virtue of Article 79(2)(c) TFEU – which prevents its systematisation within the Schengen *acquis* or, alternatively, within the AFSJ¹⁰⁶. This landscape is further complicated by four countries – namely Romania, Bulgaria, Croatia, and Cyprus – that have been denied the entry into the

¹⁰² See Chapter I.

¹⁰³ On the VIS it is interesting to see the opinion of the Council Legal Service in Council of the EU, *Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of the Member States responsible for internal Security and by Europol for the purposes of the prevention, detection and investigation of the terrorist offences and of other serious criminal offences – Schengen relevance*, 9317/06, 15 May 2006, in which it firmly maintained that the VIS should have been perceived as a development of the Schengen *acquis* covering short-stay visas.

¹⁰⁴ The Eurodac is applied by thirty-one states: all twenty-seven EU Member States plus the four Schengen Associated Countries. Nevertheless, the discussions surrounding the Eurodac negotiations in the ‘90s reveals that the relationship of the system with the Schengen *acquis* was not so clear. See, for example, the request of the Danish delegation to the Council Legal Service for further explanations on whether the draft Eurodac Regulation was Schengen relevant or not in Council of the EU, *Proposal for a Council Regulation concerning the establishment of 'Eurodac' for the comparison of fingerprints of applicants for asylum and certain other aliens*, 11683/99, Brussels, 8 October 1999, p. 1.

¹⁰⁵ See Title V of the TFEU.

¹⁰⁶ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third-country nationals - Schengen relevance*, 10768/17, Brussels, 28 June 2017.

freedom of movement area¹⁰⁷ and their partial participation in the Schengen *acquis*¹⁰⁸ bars them from accessing some large-scale IT systems and interoperability components¹⁰⁹.

The cross-cutting dimension of Regulation (EU) 2019/817 and Regulation (EU) 2019/818 risks bypassing the participation of EU States and Schengen Associated Countries in the underlying EU policies, thereby creating the possibility that the data might be accessed by unauthorised authorities. The provision of two almost identical Regulations was undertaken so as to prevent eroding the limits imposed by such an extended “variable geometry”. However, we believe that the split chosen by the co-legislators does not perfectly mirror the freedom/security dichotomy. While Regulation (EU) 2019/817 in the field of borders and visas is underpinned by Articles 16(2), 74, 77(2)(a), (b), (d) and (e) TFEU, Regulation (EU) 2019/818 in the field of police and judicial cooperation, asylum, and migration is underpinned by Articles 16(2), 74, 78(2)(e), 79(2)(c), 82(1)(d), 85(1), 87(2)(a) and 88(2) TFEU. Therefore, the Schengen *acquis* and freedom, security and justice legal bases have been merged under a sole regulation which might override the limits imposed by the founding Treaties.

¹⁰⁷ The Council of the has been procrastinating the adoption of such a relevant decision and, at the time of writing, it is not clear if or when these Member States’ external borders will be considered the frontline of the Schengen area too. See the Act concerning the conditions of accession of the Czech Republic, the Republic of Estonia, the Republic of Cyprus, the Republic of Latvia, the Republic of Lithuania, the Republic of Hungary, the Republic of Malta, the Republic of Poland, the Republic of Slovenia and the Slovak Republic and the adjustments to the Treaties on which the European Union is founded - Protocol No. 10 on Cyprus, *OJ L* 236, 23.9.2003, p. 955; the Act concerning the conditions of accession of the Republic of Bulgaria and Romania and the adjustments to the Treaties on which the European Union is founded, *OJ L* 157, 21.6.2005, pp. 203-375, and the Act concerning the conditions of accession of the Republic of Croatia and the adjustments to the Treaty on European Union, the Treaty on the Functioning of the European Union and the Treaty establishing the European Atomic Energy Community, *OJ L* 112, 24.4.2012, pp. 6-110.

¹⁰⁸ These States do not fully apply the Schengen *acquis* until the EU Council's unanimously consents them to join the Schengen enhanced cooperation. See Article 7 of the Protocol No 19, for which: ‘[...] the admission of new Member States into the European Union, the Schengen *acquis* and further measures taken by the institutions within its scope shall be regarded as an *acquis* which must be accepted in full by all States candidates for admission’ read in conjunction with Articles 330 and 331 TFEU. For Ireland (and once the United Kingdom) see Article 6(1) and (3) of Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis*, *OJ L* 131, 1.6.2000, pp. 43-47, read in conjunction with Article 4 of the Protocol No 19 just mentioned.

¹⁰⁹ Specifically, the non-participation of a Member States in a large-scale IT system should prevent it from establishing and visualising the links generated according to Article 1 of the IO Regulations as we examine *infra*.

2.1.1. The participation of Ireland, Denmark, and the Schengen Associated Countries in the interoperability Regulations

a) The participation of Ireland (and previously the United Kingdom)

Given that Ireland does not take part in the free movement project and its correlated policies – among which is included the management of external borders¹¹⁰ – but adheres to those dispositions concerning the PJCCM, the country's situation has always been challenging to manage both theoretically and practically¹¹¹. In “systems terms”, Ireland is excluded from those measures that clearly stem from the borders section – i.e., the VIS, the EES, and the ETIAS – regardless of the purpose for which the data is accessed. Accordingly, Ireland was excluded from the SIS II first-pillar alerts regulated under Regulation (EC) No 1987/2006 as it did not adhere to the underlying policy, but it could take part in the SIS II alerts on PJCCM as regulated by Council Decision 2007/533/JHA¹¹². Following this rationale, the Council Legal Service firmly excluded Ireland from the SIS II Council Regulation (EC) No 871/2004 considering that, even if that proposal was directed at amending the Convention implementing the Schengen Agreement, visa and immigration authorities could have not been granted access to the SIS II for administrative purposes. While referring to the United Kingdom, the Council Legal Service maintained:

‘[...] it does not matter if the authorities in the United Kingdom which are competent for the seizure of stolen documents and for the instigation of criminal proceedings against those seeking to misuse such documents belong to its national immigration service. What matters are the purposes for which the authorities which have access to the SIS data pursuant to the provisions of Article 101 of the Schengen Convention use such data’¹¹³.

¹¹⁰ This choice goes back to the existing travel arrangements in place between these two countries – a sort of “mini-Schengen” or Common Travel Area – as mentioned in Protocol No 20. We could affirm that these States had a permanent “provisional access” to the Schengen area, since they did not want to lift the controls at the internal borders. Under these circumstances, they will not ever be subject to second Council decision to enter SIS II alerts for refusal of entry as it is analysed *infra*.

¹¹¹ Indeed, these States not only cannot vote for the adoption of the relevant measures they do not participate to, but also should be enabled to participate in the law-making procedure if not as observers – see *mutatis mutandi* the *Opinion 1/15*, paras. 105-118, as explained *infra*.

¹¹² In this regard, the United Kingdom and Ireland's national legislation on data protection was assessed on the basis of the EU parameters as required by the DPD as it is set forth in the Council Implementing Decision (EU) 2015/215 of 10 February 2015 on the putting into effect of the provisions of the Schengen acquis on data protection and on the provisional putting into effect of parts of the provisions of the Schengen acquis on the Schengen Information System for the United Kingdom of Great Britain and Northern Ireland, *OJ L* 36, 12.2.2015, pp. 8-10. The United Kingdom could fully integrate the SIS II for law enforcement purpose only in 2015 – see “The United Kingdom connected to SIS managed by eu-LISA”, *Press Release*, 13 April 2015, available at www.eulisa.europa.eu.

¹¹³ See the Council of the EU, *Initiative of the Kingdom of Spain with a view to the adoption of a Council Regulation concerning the introduction of some new functions for the Schengen Information System[, in particular in the fight against terrorism]* (document 9407/2/02). *Initiative of the Kingdom of Spain with a view to the adoption of a*

The historical request of the United Kingdom to access the VIS for the purposes of the prevention, investigation, detection, or prosecution of serious criminal and terrorism offences through its law enforcement authorities was also rejected¹¹⁴, as:

‘[...] these two Member States do not participate in the visa provisions of the Schengen *acquis*, they are not entitled to participate in the adoption of these provisions either. Consequently, they cannot be bound by its provisions unless they choose to activate Article 4 of the Schengen Protocol (in relation to the Schengen *acquis* with respect to the Community’s visa policy) and pass the vetting procedure contained therein’¹¹⁵.

In sum, should Ireland wish to participate in the VIS, the EES, or the ETIAS, it must ask to participate in the underlying EU policy by submitting a notification to the Council and wait for its unanimous approval. However, in the case of the Eurodac¹¹⁶ and the ECRIS-TCN – that are not Schengen *acquis* systems – Ireland benefits from a full opt-in/opt-out regime¹¹⁷ and it has

Council Decision concerning the introduction of some new functions for the Schengen Information System[in particular in the fight against terrorism] (document 9408/2/02), 13713/02, Brussels, 5 November 2002, p. 13.

¹¹⁴ See their joint declaration in the Council of the EU, *Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences*, 10290/07, Brussels, 8 June 2007, p. 20.

¹¹⁵ See Council of the EU, 9317/06, Brussels, 15 May 2006. On this point, Emilio De Capitani, “The Schengen system after Lisbon: from cooperation to integration”, *ERA Forum*, No. 15, 2014, pp. 101-118, p. 110, reflects that:

‘The second trade-off was to define the Schengen system as “enhanced cooperation” between some EU Member States. It was an elegant solution designed, as the United Kingdom and Ireland would not be obliged to opt out from it. However, this definition, even if formally correct, has become somehow extravagant because, since the Treaty of Amsterdam, all new EU Member States have to accept all the Schengen *acquis*. But if an “enhanced cooperation” associates (or will sooner or later associate) 26 of 28 EU Member States, what would at the end be the exact scope of an “ordinary cooperation”?’.

¹¹⁶ However, the participation of the United Kingdom did raise concern to the Spanish delegation that insist on clarifying the position of that Member States in the Commission the Council of the EU, *Proposal for a Council Regulation concerning the establishment of “Eurodac” for the comparison of fingerprints of applicants for asylum and certain other aliens*, 10530/99, Brussels, 2 August 1999. The Spanish delegation suggested to exclude Gibraltar from its territorial scope in the following terms: ‘Were this Regulation to apply to the United Kingdom it would only apply to the territory of the United Kingdom and Northern Ireland’ – see the Council of the EU, *Proposal for a Council Regulation concerning the establishment of ‘Eurodac’ for the comparison of fingerprints of applicants for asylum and certain other aliens*, 11396/99, Brussels, 1 October 1999. The United Kingdom, in return, alleged that being the Eurodac regulation an implementation of the Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities - Dublin Convention, *OJC* 254, 19.8.1997, pp. 1-12, the extension of its territorial scope to Gibraltar was compatible with it.

¹¹⁷ See Protocol No 21, that regulates Ireland’s participation in those measures that constitute a development of the area of freedom, security and justice that are not part of the Schengen *acquis*.

exercised its opt-in through a notification as far as the Eurodac is concerned¹¹⁸, but has not done so for the ECRIS-TCN (at least at the time of writing¹¹⁹).

The main consequence of Ireland's partial participation in the Schengen *acquis* and its discretionary participation in the AFSJ is the splitting of those legislative texts that concern the entire AFSJ – i.e., the freedom section as well as the one on PJCCM¹²⁰. This was clearly reflected in Council Regulation (EU) No 1273/2012 and Council Regulation (EU) No 1272/2012 on the migration of SIS+1 to SIS II despite the fact that both Regulations were underpinned by Article 74 TFEU¹²¹. In addition, on the occasion of the adoption of the recast SIS II Regulations in 2018, the European Commission adopted not two, but three different texts¹²² as Ireland was found to not be entitled to participate in Regulation (EU) 2018/1861, and only in Regulation (EU) 2018/1862¹²³. Such an over-complicated situation is due to the establishment of a new category of alerts for the SIS II concerning the return of illegal migrants which was set forth under Regulation (EU) 2018/1860, though we believe that the SIS II alerts on refusal of entry regulated under Regulation (EU) 2018/1861 also struggle with the same question: Is illegal migration a development of the Schengen *acquis* or of the AFSJ?

¹¹⁸ See Article 3 of the Protocol No 21, establishing that the notification shall be made in a three-month period from the presentation of the legislative proposal from the European Commission to the legislators. See the Commission Decision on the Request by Ireland to accept Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), 11 December 2014, C(2014) 9310 final, *OJ L* 180, 29.6.2013, pp. 1-30.

¹¹⁹ In any case, this decision can be taken at a later stage, once the legislative measure has already been adopted, yet the enhanced cooperation procedure shall be followed – see Article 4 of Protocol No 21 that recalls Article 331(1) of the TFEU.

¹²⁰ Remarkably, also the SIRENE manual should be split in two texts following this rationale: Indeed, some of the SIS II alerts regulated therein still cannot be inserted by Ireland.

¹²¹ See the Council of the EU, *Proposal for a Council Regulation on migration from the Schengen Information System (SIS I+) to the second generation Schengen Information System (SIS II) (recast)*, 14003/12, Brussels, 20 September 2012.

¹²² See Chapter III.

¹²³ Council Decision 2004/926/EC of 22 December 2004 on the putting into effect of parts of the Schengen *acquis* by the United Kingdom of Great Britain and Northern Ireland, *OJ L* 395, 31.12.2004, pp. 70-80, granted the United Kingdom the implementation of the Schengen *acquis* in relation to police and judicial cooperation and, therefore, allowed the United Kingdom to start using the SIS II for that purposes, and the Council Implementing Decision (EU) 2020/1745 of 18 November 2020 on the putting into effect of the provisions of the Schengen *acquis* on data protection and on the provisional putting into effect of certain provisions of the Schengen *acquis* in Ireland, *OJ L* 393, 23.11.2020, pp. 3-11 – see Solenn Paulic, "L'Irlande rejoint le Système d'information Schengen", *Bulletin Quotidien Europe*, No. 12678, 16.3.2021.

Illegal migration should be presented as a “hybrid” issue, where Schengen border measures and those of freedom, security and justice overlap¹²⁴. Indeed, SIS alerts are entered not only when an irregularity stems from the illegal crossing of external borders – i.e., following a breach of the Convention implementing the Schengen Agreement –, but also when Member States’ domestic law and the norms laid down in the Return Directive breached¹²⁵, which impedes conferring on the SIS II a clear alternative position within or outside the Schengen *acquis*. Despite this, Regulations (EU) 2018/1860 and 2018/1861 are presented as developments of the Schengen *acquis* as a whole and, consequently, they exclude the participation of Ireland¹²⁶ provided that it did not opt-in to Article 96 of the Convention implementing the Schengen Agreement¹²⁷. As the Council Legal Service has clearly affirmed ‘[...] neither the United Kingdom, nor Ireland can enter or execute entry bans in the SIS, due to the fact that they do not take part in the borders part of the SIS’¹²⁸. On the occasion of the negotiations of Regulation (EU) 2018/1860, the Council Legal Service still classified return alerts as measures supporting the Schengen *acquis tout court* while affirming that: ‘[...] the absence of controls on internal borders makes it possible that persons, including third country nationals subject to return, may move from one Member State to another without being checked’¹²⁹.

Thus, the SIS II is perceived as a tool to support the identification of migrants, including those within the territories of the Member States, and to enhance the return of individuals who did not, or no longer, fulfil the conditions to enter the Schengen area¹³⁰. According to this

¹²⁴ Different scenarios may determine the illegal status of a third country national and these scenarios may represent breaches to Schengen *acquis* measures – e.g., a person illegally entering the Schengen area for a short stay – or not – e.g., a person that irregularly overstays after the expiration of a long-residence permit. In both cases the presence of the third country national within the territory of a Member State is unlawful, but the illegality has different sources: the former stems from the Schengen *acquis*, the latter from the AFSJ. Trickier would be the case of a third country national coming from a visa-exempt third country that enters the territory of a Member State legally and, once the short-stay period expires, he/she irregularly overstays in the territory. This possibility shall also be classified as an irregularity stemming from the Schengen *acquis* since the entry is justified by a short-stay permit that would have its alterego in a Schengen visa.

¹²⁵ See Article 24 of Regulation (EU) 2018/1861.

¹²⁶ See recital (60) of Regulation (EU) 2018/1861: ‘This Regulation constitutes a development of the provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC (21); Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application’, and recital (30) of Regulation (EU) 2018/1860: ‘This Regulation constitutes a development of the provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC (12); Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application’.

¹²⁷ Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis*, *OJ L* 131, 1.6.2000, pp. 43-47.

¹²⁸ See the Council of the EU, 10768/17, Brussels, 28 June 2017, p. 11.

¹²⁹ *Ibid.*, p. 14.

¹³⁰ *Ibid.*, p. 14. In the Council Legal Service’s opinion:

‘As regards the identification of a third country national subject to return within the territory of the Member States, although there is no direct link with the external borders, the objective and the scope of the measure

reading, Ireland could participate in both the return and refusal of entry alerts only if it requests to opt-in to the entire underlying EU policy on borders as the CJEU recalled: '[...] the need for coherence of [the Schengen] *acquis*, and the need – where that *acquis* evolves – to maintain that coherence'¹³¹ and maintained that measures intended as an implementation or further development of the Schengen *acquis* '[...] must be consistent with the provisions they implement or develop'¹³². Therefore, the systematisation of the SIS alerts on returns as well as on entry bans prevents Ireland from opting-in to Regulations (EU) 2018/1860 and 2018/1861 regarding the refusal of entry alerts entered following a breach of its domestic law, or the EU migration policy that does not fall under the scope of the Schengen *acquis*.

This position is inconsistent with the one taken by the Council Legal Service on the Return Directive that, although presented as a development of the Schengen *acquis* as a whole, has a clear hybrid nature as within its recitals it refers to both Council Decisions 2000/365/EC and 2002/192/EC, as well as to Protocol No 21 of the Treaty of Lisbon¹³³. The difficult wording used therein makes us wonder whether Ireland could or could not participate in this measure and, if it did, which procedure it should follow. According to the Council Legal Service, Ireland was granted the right to opt-in to the Return Directive only with regard to returned third country nationals failing to comply with the conditions of entry, stay, or residence established under its domestic law while excluding “Schengen’s irregularities”¹³⁴. The same conditions were applied under Council Directive 2001/40/EC on the mutual recognition of decisions on the expulsion

should be the same. It primarily makes sense to apply also this provision to those third country nationals who have entered the Schengen area without internal border controls and who have moved and been found in the territory of other Member States within that area’.

¹³¹ See C-482/08, *United Kingdom v Council*, paras. 48 to 58.

¹³² In the same line, see C-77/05, *United Kingdom v Council*, paras. 60 and 61.

¹³³ See recital (26) of the Return Directive:

‘To the extent that it applies to third-country nationals who do not fulfil or who no longer fulfil the conditions of entry in accordance with the Schengen Borders Code, this Directive constitutes a development of provisions of the Schengen *acquis* in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis* (6); moreover, in accordance with Articles 1 and 2 of the Protocol on the position of the United Kingdom and Ireland annexed to the Treaty on European Union and to the Treaty establishing the European Community, and without prejudice to Article 4 of the said Protocol, the United Kingdom is not taking part in the adoption of this Directive and is therefore not bound by it in its entirety or subject to its application’.

Recital (27) of the Return Directive:

‘To the extent that it applies to third-country nationals who do not fulfil or who no longer fulfil the conditions of entry in accordance with the Schengen Borders Code, this Directive constitutes a development of provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC of 28 February 2002 concerning Ireland’s request to take part in some of the provisions of the Schengen *acquis* (7); moreover, in accordance with Articles 1 and 2 of the Protocol on the position of the United Kingdom and Ireland annexed to the Treaty on European Union and to the Treaty establishing the European Community, and without prejudice to Article 4 of the said Protocol, Ireland is not taking part in the adoption of this Directive and is therefore not bound by it in its entirety or subject to its application’.

¹³⁴ See the Council of the EU, 10768/17, 28 June 2017.

of third country nationals¹³⁵ and Council Decision 2004/191/EC, which set forth the criteria for repaying the costs incurred by the enforcing Member State¹³⁶. For the time being, Ireland has not opted-in to the Return Directive and, if it decided to do so, it should be prevented from opting into Schengen dispositions unless it adheres to the underlying EU policy based on Article 79(2)(c) TFEU¹³⁷. Conversely, Ireland is authorised to opt-in to those return alerts that represent an execution of the EU policy on illegal migration through the AFSJ and that do not constitute a development of the Schengen *acquis*¹³⁸. Today, it is unclear to us whether these conditions will be respected, as these peculiarities are not taken into account either in Regulation (EU) 2018/1860 or in Regulation (EU) 2018/1861.

Similar criticism can be directed against the IO Regulations that do not distinguish between Schengen and AFSJ systems while framing both legislative texts as a development of the Schengen *acquis*¹³⁹. This split does not respect the nature of the Eurodac and the ECRIS-TCN that are framed under Regulation (EU) 2019/818, though some clarification on their freedom, security and justice nature can be seen in Recitals (74) and (75) of Regulation (EU) 2019/818¹⁴⁰. Here, the co-legislators took note of the fact that the United Kingdom was bound by Regulation (EU) 2019/818 as it opted-in to Regulation (EU) 2018/1862 as far as the SIS alerts on PJCCM were concerned and it also notified its intention to participate in AFSJ systems— namely the Eurodac¹⁴¹ and the ECRIS-TCN¹⁴². In its case, Ireland was deemed not to be bound by

¹³⁵ See the Council Directive 2001/40/EC on the mutual recognition of decisions on the expulsion of third country nationals, *OJ L* 149, 2.6.2001, p. 34.

¹³⁶ See the Council Decision 2004/191/EC of 23 February 2004 setting out the criteria and practical arrangements for the compensation of the financial imbalances resulting from the application of Directive 2001/40/EC on the mutual recognition of decisions on the expulsion of third-country nationals, *OJ L* 60, 27.2.2004, pp. 55-57, in which the United Kingdom opted-in according to its recital (8) that sounds as follow:

‘In accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland, annexed to the Treaty on the European Union and to the Treaty establishing the European Community, the United Kingdom has notified its wish to take part in the adoption and application of this Decision. To the extent that this Decision also implements the provisions of Article 24 of the Schengen Convention, in accordance with Article 7 of Directive 2001/40/EC, it does not affect the United Kingdom’.

¹³⁷ Which must be agreed unanimously by the Council by virtue of its Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis*, *OJ L* 64, 7.3.2002, pp. 20-23.

¹³⁸ It shall be highlighted that the interpretation of the SIS II Regulation (EU) 2018/1860 as a full Schengen *acquis* measure instead of a hybrid act would exclude the Schengen Associated Countries as far as SIS II alerts on the EU return policy are concerned.

¹³⁹ See recitals (73)-(78) of Regulation (EU) 2019/817 and recitals (77)-(82) of Regulation (EU) 2019/818.

¹⁴⁰ Recitals (74) and (75) of Regulation (EU) 2019/818 correctly refer to Protocol No 21, as far as Eurodac and ECRIS-TCN are concerned.

¹⁴¹ Council of the EU, *Notification from the United Kingdom concerning its intention to take part in the adoption of the Council Regulation (EC) concerning the establishment of “EURODAC” for the comparison of fingerprints of applicants for asylum and certain other aliens*, 11870/1/99 REV 1, Brussels, 18 October 1999, and recital (52) of the 2013 Eurodac recast Regulation.

¹⁴² Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing the conditions for accessing the other EU information systems and amending Regulation (EU) 2018/1862 and Regulation (EU) yyyy/xxx [ECRIS-TCN] - Opt-in by the United Kingdom*, 8809/19, Brussels, 24 April 2019.

Regulation 2019/818 since, although taking part in the SIS Regulation 2018/1862, it did not state its intention to participate in the interoperability norms concerning the Eurodac and the ECRIS-TCN¹⁴³. In the specific case of the ECRIS-TCN, Ireland should have opted-in to this system before, or alongside, Regulation (EU) 2019/818. Recital (75) of Regulation (EU) 2019/818 states that:

‘[...] Since it is not possible, under these circumstances, to ensure that this Regulation is applicable in its entirety to Ireland, as required by Article 288 of the TFEU, Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application, without prejudice to its rights under Protocols No 19 and No 21’.

Such an approach does not reflect Ireland’s opting-in to the SIS Regulation (EU) 2018/1862 and its subsequent developments according to Council Decision 2002/192/EC. The co-legislators do not ignore the issue, going so far as to affirm that ‘[i]nsofar as its provisions relate to SIS as governed by Regulation (EU) 2018/1862, Ireland could, in principle, take part in this Regulation, in accordance with Article 5(1) of Protocol No 19 on the Schengen *acquis* integrated into the framework of the European Union, annexed to the TEU and to the TFEU, and Article 6(2) of Council Decision 2002/192/EC’, yet, the merging of PJCCM, migration, and asylum legal bases bars Ireland from participating in the Regulation (EU) 2019/818. Besides, the EU legislator has restricted Ireland’s participation in Regulation (EU) 2019/817¹⁴⁴ if the “hybrid nature” between the Schengen *acquis* and the AFSJ of the SIS Regulations (EU) 2018/1861 and (EU) 2018/1860 is taken into account. *A fortiori* the co-legislators did not include Regulation (EU) 2018/1860 in the framework of the interoperability of large-scale IT systems established by Regulation (EU) 2019/818 as we expected, this was due to the fact that Article 79(2)(c) TFEU was not taken into consideration when issuing Regulation (EU) 2019/817¹⁴⁵. The combining of Regulation (EU) 2018/1860 and Regulation (EU) 2018/1861 following Regulation (EU) 2019/817 is problematic as even if both Regulations were underpinned by the EU competence on the prevention of, and combat against, illegal migration set forth in Article 79(2)(c) TFEU, Regulation (EU) 2018/1861 is also underpinned by Article 77(2)(b) and (d) TFEU. Provided that Article 79(2)(c) TFEU appears only under the legal framework established by Regulation (EU) 2019/818, the co-legislators have opted to classify the SIS alerts on refusal of entries and on return as measures stemming from the Schengen *acquis tout court*, preventing Ireland from freely opting-in to those SIS II alerts that are not the result of a “Schengen irregularity”.

¹⁴³ Ireland opted-in Eurodac according to the Commission Decision on the Request by Ireland, C(2014) 9310 final, OJ L 180, 29.6.2013, pp. 1-30.

¹⁴⁴ See recitals (78) and (79) of Regulation (EU) 2019/817.

¹⁴⁵ See Article 3 of Regulation (EU) 2019/817.

These considerations lead us to conclude that the “sister solution” created by the co-legislator does not fully respect the dichotomy of Schengen *versus* AFSJ measures imposed by the founding Treaties. Specifically, Ireland is denied access to, and the usage of, data it should be entitled to by virtue of its limited discretion in opting-in/opting-out measures stemming from the Schengen *acquis*. However, this solution guarantees that Ireland cannot access Schengen alerts that it is not entitled to issue. The adoption of a third interoperability Regulation establishing a framework for the interoperability of the Eurodac and the ECRIS-TCN could have softened our criticism, as Ireland could have opted-in to these systems. Yet, even if this were done, the issues stemming from the “hybrid nature” of the SIS alerts would most likely have been ignored by the co-legislators as, in practice, it is very difficult to distinguish between Schengen and AFSJ alerts.

b) Denmark’s participation

According to Protocol No 22¹⁴⁶, within a period of six months Denmark can communicate whether it wants to take part in a measure adopted as a development of the Schengen *acquis* and, as a consequence, commit to integrating it in its national law by virtue of an international agreement. In the case of the SIS, Denmark communicated its intention to participate in the entire system on 29 April 2019¹⁴⁷. Although its notification for adopting the VIS Regulation has not been published, the official page of the Commission states that Denmark also incorporated the VIS Regulation and the VIS LEA Decision into its national laws. However, a new notification is expected regarding the revised Regulation¹⁴⁸. Furthermore, Denmark

¹⁴⁶ See Protocol No 22.

¹⁴⁷ See the Council of the EU, *Schengen Information System (SIS) – Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) for the return of illegally staying third-country nationals – Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006 – Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU - Notification from Denmark*, 8913/19, Brussels, 29 April 2019.

¹⁴⁸ See recital (59) of the Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System, *OJ L* 248, 13.7.2021, pp. 11-87, and recital (13) of Regulation (EU) 2021/1133 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EU) No 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 and (EU) 2019/818 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the Visa Information System, PE/45/2021/INIT, *OJ L* 248, 13.7.2021, pp. 1-10; the latter referring to the dispositions concerning Regulation (EU) 2018/1862 only.

notified its willingness to participate in the EES¹⁴⁹ and in the ETIAS¹⁵⁰. Provided that Denmark's willingness to participate in the AFSJ is also limited to the intergovernmental framework – and that it has not adhered to the opt-in/opt-out regime established for Ireland – its participation in EU acts is (arguably) guaranteed thanks to a treaty concluded in 2006 in order to allow Denmark access to the Eurodac¹⁵¹, however, at the time of writing, this is not the case for the ECRIS-TCN.

Accordingly, both IO Regulations establish that Denmark can communicate its willingness to participate in Regulation (EU) 2019/817¹⁵² and Regulation (EU) 2019/818¹⁵³ within a period of six months once Denmark has decided whether it will implement the Regulations in its national law. Yet, Regulation (EU) 2019/818 specifies that Denmark's notification is limited to those provisions that '[...] relate to SIS as governed by Regulation (EU) 2018/1862' since these are only built upon the Schengen *acquis*. No specification has been given as far as the Eurodac and the ECRIS-TCN are concerned, though Denmark participates in the former and may in future participate in the latter by concluding an international treaty with the EU.

¹⁴⁹ See the Council of the EU, *Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 - Notification from Denmark*, 10999/18, Brussels, 10 July 2018.

¹⁵⁰ Unfortunately, Denmark's notification is not published.

¹⁵¹ On 1 April 2006 a special Agreement entered into force between the European Community and the Kingdom of Denmark on the latter's special position and on the extension of the Dublin and Eurodac Regulations to it – see the Agreement between the European Community and the Kingdom of Denmark on the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in Denmark or any other Member State of the European Union and "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention, *OJ L 66*, 8.3.2006, p. 37. In the same sense, a special Protocol entered into force on 21 February 2006, regulating the relations between Denmark, of the one part, and Norway and Iceland, of the other part, on the same issue. This was enriched by a further Protocol annexed to the Dublin/Eurodac agreement between the EU Switzerland and Liechtenstein so that Denmark could access the system – see the Council of the EU, *Signature of a protocol on Denmark's participation in the Dublin/Eurodac agreement with Switzerland and Liechtenstein*, 7059/08, Brussels, 28 February 2008.

¹⁵² Recital (73) of Regulation (EU) 2019/817:

'In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law'.

¹⁵³ Recital (77) of Regulation (EU) 2019/818:

'In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation, insofar as its provisions relate to SIS as governed by Regulation (EU) 2018/1862, builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law'.

In the lack of any express provision on the participation of Denmark in the Eurodac and the ECRIS-TCN, and although Denmark's participation is sealed by an international agreement, the adoption of a third interoperability Regulation on freedom, security, and justice systems might have been useful to clarify that Denmark is acting under different legal frameworks depending on whether the measure at stake constitutes a development of the Schengen *acquis* or not and, specifically, that a six-month notification is not needed as far as the Eurodac and the ECRIS-TCN are concerned. Besides, no specification on the "hybrid nature" of the SIS alerts on refusal of entry or the ones on return has been inserted. The interpretation given by the co-legislators of Regulations (EU) 2018/1861 and (EU) 2018/1860 facilitates Denmark's participation in the above-mentioned SIS instruments through a notification within six months from the Council's decision instead of the mere conclusion of an international treaty. However, our analysis leads us to conclude that such a procedure should be only valid for the SIS II alerts that can be considered as "Schengen irregularities" and not for those regarding freedom, security and justice.

c) The participation of Iceland, Norway, Switzerland, and Lichtenstein

Schengen Associated Countries were allowed to join the EU as far as the Schengen *acquis* is concerned, as they had already adhered to the Convention implementing the Schengen Agreement before its institutionalisation¹⁵⁴. Their participation was sealed through the conclusion of four international treaties between the European Community and Norway, Iceland, Lichtenstein, and Switzerland respectively¹⁵⁵. Therefore, these countries are not only bound by the Schengen *acquis* as integrated in EU Law, but are also subjected to the measures adopted by the EU legislator on the basis of such an *acquis*¹⁵⁶. Schengen Associated Countries

¹⁵⁴ See Article 6 of Protocol No 19.

¹⁵⁵ See the: Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latter's association with the implementation, application and development of the Schengen *acquis*, *OJ* 176/36, 10.7.1999, and the Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis*, *OJ* L 176, 10.7.1999, pp. 31-33; the Council Decision of 28 January 2008 on the conclusion on behalf of the European Union of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, *OJ* L 53, 27.2.2008, pp. 50-51, though Articles 1 to 4 of the Council Decision 1999/437/EC with Iceland and Norway were made applicable to Switzerland already in, and the Council Decision 2011/842/EU of 13 December 2011 on the full application of the provisions of the Schengen *acquis* in the Principality of Liechtenstein, *OJ* L 334, 16.12.2011, pp. 27-28.

¹⁵⁶ See the Annexes to the relevant treaties mentioned in the previous note. In the daily life of the institutions, Schengen Associated Countries do not fully participate in the law-making procedure: they observe the negotiations of the legislative measures within the EU Council, without being granted the right to vote on the European Commission's proposals; in the same line, they are invited to assist to the European Commission's committees and expert groups, and they are notified once the measures have been adopted. On that moment, Schengen

are part of the large-scale IT systems that constitute a development of the Schengen *acquis*, namely the VIS¹⁵⁷, the EES, the ETIAS, and the SIS II¹⁵⁸. Conversely, as far as the non-Schengen systems are concerned, the Schengen Associated Countries must conclude international treaties with the EU to participate in them and, at the time of writing, they have done so only with regard to the Dublin Regulation for the Eurodac¹⁵⁹, while no agreement has been signed to participate in the ECRIS-TCN.

Provided that the co-legislators classify the entirety of Regulation (EU) 2019/817 as a development of the Schengen *acquis*, the Schengen Associated Countries' participation is deemed to be covered by the correspondent association agreements concluded for the implementation, application, and development of the Schengen *acquis*¹⁶⁰. Conversely, Regulation (EU) 2019/818 circumscribes the Schengen nature of its dispositions that only refer to the SIS Regulation (EU) 2018/1862¹⁶¹ and omits any reference to their participation in the Eurodac and the ECRIS-TCN. The existing considerations made for Ireland and Denmark – and previously for the United Kingdom – are valid here as well since: first, the co-legislators have not respected Protocol No 19 with the Schengen Associated Countries as far as the SIS alerts on refusal of entries and on return are concerned, as these should be regulated by two different legal frameworks; second, the co-legislators have not clarified the terms under which the Schengen Associated Countries participate in Regulation (EU) 2019/818. In the latter case, no reference is made to freedom, security and justice systems that they are accessing, or might access in the future. A final remark should be made regarding Norway and Iceland since these

Associated Countries are given a six-month period to notify whether they want to adopt the measure or not. However, in case of refusal of any measure developing the Schengen *acquis*, the underlying agreement would terminate unless the Mixed Committee establishes otherwise. In other words, Schengen Associated Countries have to accept the measures developing the Schengen *acquis* to continue participating in the Schengen enhanced cooperation.

¹⁵⁷ See the: Council Decision 2008/421/EC of 5 June 2008 on the application of the provisions of the Schengen *acquis* relating to the Schengen Information System in the Swiss Confederation, *OJ L* 149, 7.6.2008, pp. 74-77, and the Council Decision 2011/352/EU of 9 June 2011 on the application of the provisions of the Schengen *acquis* relating to the Schengen Information System in the Principality of Liechtenstein, *OJ L* 160, 18.6.2011, pp. 84-87.

¹⁵⁸ See the Council of the EU, - *Notification from Switzerland*, 5409/19, 15 January 2019; the - *Notification from Liechtenstein*, 6696/19, Brussels, 27 February 2019, and the Council of the EU - *Notification from Iceland*, 6750/20, Brussels, 11 March 2020. The notification from Norway is not published.

¹⁵⁹ See the: Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland, *OJ L* 53, 27.2.2008, p. 5; Agreement between the European Community and the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Iceland or Norway, *OJ L* 93, 3.4.2001, p. 40, and the Protocol between the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a member State or in Switzerland, *OJ L* 160, 18.6.2011, p. 39.

¹⁶⁰ Recitals (80)-(82) of Regulation (EU) 2019/817.

¹⁶¹ Recitals (76)-(78) of Regulation (EU) 2019/818.

states are excluded from the SIS alerts of Regulation (EU) 2018/1862 concerning the European Arrest Warrant, which reflects their non-participation in the corresponding enhanced cooperation¹⁶², but no specification has been made in this regard.

2.1.2. The participation of Member States that do not fully apply the Schengen *acquis*: The cases of Romania, Bulgaria, Croatia, and Cyprus

Since the Amsterdam Treaty entered into force, candidate states that wish to become Member States of the EU must accept the entire Schengen *acquis* that requires the acceptance of:

- the common visa issuing policy;
- the common asylum granting policy;
- the operational readiness of the N-SIS II and its interoperability with the C- SIS;
- the police cooperation;
- the protection of external land, sea, and air borders, and
- the compliance with the EU level of data protection requirements¹⁶³.

The incorporation of the entire Schengen *acquis*, especially the full entry into operation of the large-scale IT systems, is quite a long procedure that is monitored through the SCH-EVAL¹⁶⁴ and ends up with a Council Decision that unanimously agrees the accession of the Member State to the Schengen enhanced cooperation – i.e., the lifting of controls at internal borders¹⁶⁵. Indeed, the implementation of the systems puts the data stored therein at the disposal of new Member States and the latter are required to comply with the EU standards on the protection of personal data before being able to make full use of them. Meanwhile, the Council of the EU usually grants a new State “provisional access” to these systems and, specifically, to

¹⁶² See the contribution of the Spanish delegation in the Council of the EU, *Proposal for a draft Council Decision on the Establishment, Operation and Use of the Second Generation Schengen Information System (SIS II) – Revised proposal*, 5710/4/06 REV 4 ADD 1, Brussels, 17 July 2006.

¹⁶³ These conditions are set forth in the association agreement that the EU celebrates with new candidate states. For the big enlargement of 2003 – see the Council of the EU, *Council Decision on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Czech Republic, the Republic of Estonia, the Republic of Latvia, the Republic of Lithuania, the Republic of Hungary, the Republic of Malta, the Republic of Poland, the Republic of Slovenia and the Slovak Republic*, 8611/07, Brussels, 20 April 2017.

¹⁶⁴ Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen, *OJ L* 295, 6.11.2013, pp. 27-37.

¹⁶⁵ Generally, when a new Member State joins the EU it is progressively bound by the Schengen *acquis* measures according to conditions set forth in the accession treaty and the subsequent decisions agreed in the Council, with the exceptions of those Member States that do not form part of the Schengen enhanced cooperation, namely Ireland, Croatia, Cyprus, Bulgaria and Romania – previously also the United Kingdom.

the SIS refusal of entry alerts for law enforcement purposes¹⁶⁶. Provided that the Council may procrastinate over this decision for political reasons, Member States can be locked in a 'provisional' position that prevents them from properly using the systems for a considerable time.

For various political reasons Romania, Bulgaria¹⁶⁷, Croatia¹⁶⁸, and Cyprus¹⁶⁹ have not been allowed to lift controls at their internal borders, this translates into the existence of four different legal frameworks as far as large-scale IT systems are concerned¹⁷⁰. In 2011, the Council concluded that the conditions relating to air borders, sea borders, land borders, police cooperation, data protection, the SIS, and visas had been satisfactorily fulfilled¹⁷¹ by Bulgaria and Romania¹⁷². Yet, the subsequent SCH-EVAL revealed some tension regarding the standards adopted on the protection of personal data, triggering enhanced scrutiny by the European Parliament¹⁷³. Unlike Bulgaria and Romania, Croatia has not yet fulfilled the SCH-EVAL¹⁷⁴ while Cyprus has been granted a temporary derogation for entering the Schengen area

¹⁶⁶ It is eu-LISA that supports these new states to implement the systems. While the SIS is a *condicio sine qua non* Member States can lift the controls at the internal borders, the other is used by the new Member States as far as their operational implementation has successfully ended. It is expected that in the future all these systems will be evaluated under the SCH-EVAL mechanism to monitor their effective implementation.

¹⁶⁷ Bulgaria and Romania entered the EU in 2005 with the Act concerning the conditions of accession of the Republic of Bulgaria and Romania and the adjustments to the Treaties on which the European Union is founded, *OJ L* 157, 21.6.2005, pp. 203-375.

¹⁶⁸ Croatia has been a Member State of the EU since 2011 according to the Decision of the Council of the European Union of 5 December 2011 on the admission of the Republic of Croatia to the European Union, *OJ L* 112, 24.4.2012, pp. 6-110.

¹⁶⁹ Cyprus accessed the EU in 2003 but has a temporary derogation for entering the Schengen area. See the Act concerning the conditions of accession of the Czech Republic, the Republic of Estonia, the Republic of Cyprus, the Republic of Latvia, the Republic of Lithuania, the Republic of Hungary, the Republic of Malta, the Republic of Poland, the Republic of Slovenia and the Slovak Republic and the adjustments to the Treaties on which the European Union is founded – Protocol No 10 on Cyprus, *OJ L* 236, 23.9.2003, pp. 955-955.

¹⁷⁰ See also *infra* as far as the multiple identity detection proceeding is concerned.

¹⁷¹ See the European Parliament resolution of 11 December 2018 on the full application of the provisions of the Schengen acquis in Bulgaria and Romania: abolition of checks at internal land, sea and air borders (2018/2092(INI)), *OJ C* 388, 13.11.2020, pp. 18-21.

¹⁷² On the political background that is preventing those States to fully apply the Schengen *acquis* see Tomasz Dąbrowski, "The political complications of including Bulgaria and Romania in the Schengen Area", *Analyses*, 22.09.2021, available at www.osw.waw.pl.

¹⁷³ See the Council of the EU, *European Parliament plenary session on 15 June 2010 in Strasbourg on the draft Council decision on the application of the provisions of the Schengen acquis relating to the Schengen Information system in the Republic of Bulgaria and Romania*, 11263/10, Brussels, 16 June 2010.

¹⁷⁴ See the Council of the EU, *Draft Council Decision on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Republic of Croatia*, 8056/17, Brussels, 7 April 2017, in which following the evaluation of 2016 Croatia was deemed to accomplish the evaluation on the legislative measures in place for the protection on personal data. However, Croatia's compliance with the Schengen *acquis* is closely scrutinised by the Ministries of Interior – see "Les États membres de l'UE devraient terminer l'année sans réaliser de percée sur le Pacte 'Asile et migration'", *Bulletin Quotidien Europe*, No. 12848, 8.12.2021: 'Les ministres devraient aussi être invités jeudi à adopter des conclusions sur le respect intégral par la Croatie de l'acquis Schengen, conclusions qui nécessitent l'unanimité et qui ouvriraient la voie à une décision sur l'adhésion à la zone de libre circulation', and the Council green light is expected to come soon as announced in "Le ministre de l'Intérieur slovène croit en une accession rapide de la Croatie à l'espace Schengen", *Bulletin Quotidien Europe*, No. 12850, 10.12.2021.

as its territory is partially occupied by the Turks¹⁷⁵. Therefore, Bulgaria, Romania, Croatia, and Cyprus fully participate in the Eurodac, the ETIAS and the ECRIS-TCN, while some nuances must be highlighted as far as the SIS, the VIS, and the EES are concerned.

Bulgaria and Romania have been exceptionally allowed to issue SIS refusal of entry alerts since 2018, when they started make full use of the system. Croatia, can use the SIS for issuing alerts on PJCCM, but it cannot issue refusal of entry alerts – even if it is able to see and execute them in accordance with its national law. The difficult situation affecting Cyprus¹⁷⁶ prevents it from connecting to the SIS at all, but the country has started testing the system for PJCCM alerts with the support of eu-LISA. As soon as Cyprus passes the SCH-EVAL, a Council Decision should allow it to lift its controls at the internal borders and to issue refusal of entry alerts. From that moment on, Cyprus will be granted access to the VIS¹⁷⁷ and the EES will be implemented at the sea and air borders.

The application of the Schengen *acquis* by Romania, Bulgaria, Croatia, and Cyprus and, specifically, the EES's scope of application, gave rise to an interesting debate on the delimitation of the EU external borders in the light of Article 6 of the Schengen Borders Code¹⁷⁸. On this occasion, the Council Legal Service clarified that Bulgaria, Romania, Croatia, and Cyprus shall be considered as Schengen states, regardless of the fact that these Member States would continue implementing checks at their internal borders without taking part in the Visa Code until a Council decision allows them to do so¹⁷⁹. In practical terms, a harmonised calculator applicable to all Schengen states should have been created in order to compute how

¹⁷⁵ Cyprus does not have control on its own territory, nor on the corresponding internal border which prevents it to fully participate in the Schengen *acquis* – see the Council of the EU, *Answers to the additional questionnaire addressed to the new Member States related to - Schengen Information System - Prior consultation*, 5602/06 ADD 1 DCL 1, Brussels, 24 May 2018.

¹⁷⁶ See “Les élus de la commission des Libertés civiles du PE saisis des difficultés de Chypre à gérer les flux de migrants”, *Bulletin Quotidien Europe*, No. 12936, 22.4.2022, advancing an agreement among Cyprus, the European Commission, and the Union agencies' EUAA, EBCG Agency, and Europol to enhance Cyprus' capacity to welcome asylum seekers.

¹⁷⁷ See the Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between the Member States on short-stay visas*, 9423/07 ADD 1, 29 May 2007, that testifies the expression of interest made by Cyprus on participating in the system.

¹⁷⁸ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System - The calculation of the duration of stay in the framework of the automated calculator*, 11893/16, Brussels, 9 September 2016.

¹⁷⁹ See the Council of the EU, *Proposal for a Regulation establishing an Entry/Exit System (EES) - Territorial scope of application of the EES in the light of Article 6(1) of the Schengen Borders Code for the purpose of calculating the short-stay (90 days in any 180-day period)*, 3491/16, Brussels, 19 October 2016.

permanent an individual's stay was in these territories¹⁸⁰. Furthermore, these Member States must implement the EES not only at their external borders, but also at their internal ones¹⁸¹.

As Bulgaria and Romania's borders are EU borders, but the two States are not fully implementing the Schengen *acquis*, their particular situation required specific temporary provisions for the implementation of the EES until they are granted full access to the Schengen area. As a result of these provisions, Romania and Bulgaria will fully implement the EES at their sea and air borders, but their land-shared borders will be subject to specific regimes depending on whether the neighbouring countries apply the Schengen *acquis* or not. Romania and Bulgaria will not deploy the EES at those land-borders that are shared with Member States that fully implement the Schengen *acquis* – i.e., Hungary and Greece. In these cases, only the latter will record the entries to and exits from the Schengen area. Yet, the use of the EES is “provisional” and it will cease as soon as Bulgaria and Romania fully apply the Schengen *acquis*. Also, biometric data will not be registered in the EES and the records will be restricted to alphanumeric data only. With respect to the other territorial borders that form the EU's external frontline, Romania and Bulgaria will fully operate the EES. The situation is further complicated by the fact that Romania and Bulgaria also share their own frontline: Today, their borders are internal borders between two Member States that do not fully apply the Schengen *acquis*, as a result they will fully operate the EES. Although highly improbable, the scenario in which these two Member States have access to the Schengen area at different times should be considered. In this case, their land-borders would become an EU internal border between a Member State fully implementing the Schengen *acquis* and a Member State not fully

¹⁸⁰ Indeed, the question on whether a short-stay should have computed also the individual's permanence in these territories fueled the political debate on the long-awaited participation of these four Member States in the Schengen *acquis*. Confront the Bulgarian comments to the EES Proposal in the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*, 8518/16, Brussels, 4 May 2016, as well as the Romanian note in Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*, 8421/16, Brussels, 2 May 2016, and Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*, 9387/16, Brussels, 26 May 2006.

¹⁸¹ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of, entry data of third country nationals crossing the external borders of Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011 - Explanation of the functioning of Article 3a of the EES proposal*, 15351/16, Brussels, 8 December 2016.

implementing it, so the former should use the EES *vis-à-vis* the latter. On the other hand, if Bulgaria and Romania simultaneously access the Schengen area, then, the land-border they share will become an EU internal border where checks are suppressed.

Another important feature indispensable to the implementation of the EES is the ability to consult the VIS to perform the automated checks between the data stored in the two systems, for which purpose Bulgaria, Romania¹⁸², Croatia, and Cyprus¹⁸³ should be granted “passive” access to the VIS – i.e., a consultation right that prevents them from entering the corresponding files. Yet, the positions of Croatia and Cyprus differ slightly from those of Bulgaria and Romania. First, Croatia is not using the VIS and will not use the EES until it complies with the SCH-EVAL. If the Council grants Croatia “passive access to the VIS”, then, Croatia should also be able to implement the EES under an exceptional regime according to which: it will fully use the EES for its sea and air borders, while at the land borders Slovenia and Hungary will register the entry and exit of individuals without collecting biometrics. As is the case with Bulgaria and Romania, Croatia shares EU borders with Member States that fully apply the Schengen *acquis* – namely Slovenia and Hungary. Nevertheless, since Croatia is already paving its way to full implementation of the SIS, it seems reasonable to think that the Council will grant it full access to the systems when it joins the Schengen area, avoiding any half-way regime. As far as Cyprus is concerned, this Member State has been granted access to the VIS¹⁸⁴, while the EES will be provided at the sea and air borders as soon as it fulfils the SCH-EVAL. Until adoption of the SCH-EVAL is successful, Croatia and Cyprus will continue “stamping passports”¹⁸⁵ with third country nationals being subjected to a regime of reciprocity

¹⁸² See the Council of the EU, *Council Decision (EU) 2017/1908 of 12 October 2017 on the putting into effect of certain provisions of the Schengen acquis relating to the Visa Information System in the Republic of Bulgaria and Romania* (OJ L 269, 19.10.2017, p. 39–43), and the *Council Decision on the putting into effect of certain provisions of the Schengen acquis relating to the Visa Information System in the Republic of Bulgaria and Romania - Adoption*, 12411/17, Brussels, 5 October 2017, that testifies that apart from the political agreement forged in the Council decision, Bulgaria and Romania should have been successfully passed the testing phase.

¹⁸³ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011 Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 2016/399 as regards the use of the Entry/Exit System - Territorial scope of the application of the EES and the calculation of the duration of the short-stay - guidance for further work*, 5565/17, Brussels, 24 January 2017.

¹⁸⁴ See the Council of the EU, 9423/07 ADD 1, Brussels, 29 May 2007, that testifies the expression of interest made by Cyprus on participating in the system.

¹⁸⁵ See the reaction of Croatia here Council of the EU, *Draft Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System (first reading) - Adoption of the legislative act = statements*, 14091/1/17 REV 1 ADD 1, 15 November 2017, that found the “solidarity “of Slovenia here Council of the EU, *Draft Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law*

as far EU citizens are concerned¹⁸⁶. Such a privileged *status* has been granted to the EU Member States using the VIS since 2014 and consists of controlling individuals at the external borders on the basis of the unilateral recognition by Bulgaria, Croatia, Cyprus, and Romania of certain documents as equivalent to their national visas for transit through or intended short-stays in their territories – i.e., not exceeding ninety days in a period of one hundred eight days. This regime authorised the four Member States to unilaterally recognise the documents issued by the Member States fully implementing the Schengen *acquis* and gave Croatia the right to recognise certain documents issued by the Member States, including Bulgaria, Romania, and Cyprus, as equivalent to its national visas in order to speed up the controls at Croatia's external borders. Therefore, these Member States are currently adopting a regime of the one-way free movement of individuals: EU visa-holders can enter Romania, Bulgaria, Croatia, and Cyprus without requiring a national visa, but there is no reciprocity for Romania, Bulgaria, Croatia, and Cyprus' visa holders to enter the Schengen area. As a result, this situation still requires these Member States to maintain internal border checks¹⁸⁷.

As we will show below, the fact that Bulgaria, Romania, Croatia, and Cyprus do not fully apply the Schengen *acquis* impacts the IO Regulations, not only because its technical configuration must respect their participation in the underlying large-scale IT systems, but also because the impossibility of inserting or modifying an individual file in the systems prevents them from triggering the multiple identity detection procedure regulated by Article 21 of the IO Regulations. The belief that there is “data loss” in terms of the links between the files stored in the CIR¹⁸⁸ could potentially create a turning point in favour of the full adherence of Member States to the AFSJ and, consequently, towards the progressive flattening of the different needs stemming from the burden of variable geometry.

enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (first reading) - Adoption of the legislative act = statements, 14092/1/17 REV 1 ADD 1 14092/1/17 REV 1 ADD 1, Brussels, 15 November 2017 - in reality, Slovenia worried about the financial costs that the temporary implementation of the EES at the internal borders would have caused.

¹⁸⁶ See the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of, entry data of third country nationals crossing the external borders of Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011. Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 2016/399 as regards the use of the Entry/Exit System - Mandate for negotiations with the European Parliament*, 6572/17 COR 1, Brussels, 2 March 2017.

¹⁸⁷ The situation is tense since these countries also contribute to the budget for the systems – see the Council of the EU, *Draft Council Decision amending the Decision of the Executive Committee set up by the 1990 Schengen Convention, amending the Financial Regulation on the costs of installing and operating the technical support function for the Schengen Information System (C.SIS)*, 13381/09, Brussels, 30 September 2009.

¹⁸⁸ See *infra*.

2.2. A new IT infrastructure for large-scale IT systems: The components of interoperability

The IO Regulations ensure the ‘fast, seamless, systematic and controlled access to the information’ by the Member States’ authorities and Union agencies with access to the underlying IT systems. The need for this assurance finds its rationale in the new infrastructure¹⁸⁹ the IO Regulations provide for EU large-scale IT systems. From the studies conducted by eu-LISA, the interoperability architecture should have been chosen from among the following three options¹⁹⁰:

1. continuation, enabling the direct connection of large-scale IT systems with one another;
2. integration, allowing the connection of large-scale IT systems through a sole integration layer, or
3. unification, proposing a common interoperable platform within which all components and large-scale IT systems could operate.

The preferred option was that of unification that, although inserting ‘an extra component’, it would have allowed ‘[...] the number of connections between systems [to] increase linearly according to the number of connected systems’¹⁹¹.

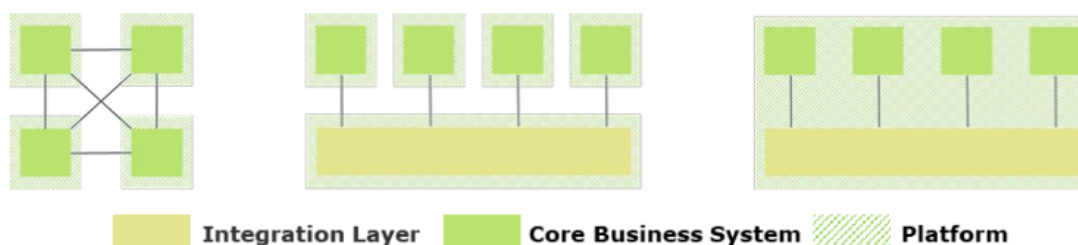


Figure 2 Architecture options for interoperability – Source: eu-LISA, Elaboration of a Future Architecture for Interoperable IT Systems at eu-LISA, Tallin, 2019.

¹⁸⁹ Giovan Francesco Lanzara, “The Circulation of Agency in Judicial Proceedings: Designing for Interoperability and Complexity”, in Francesco Contini and Giovan Francesco Lanzaraat, *The Circulation of Agency in E-Justice*, op. cit., pp. 3-32, p. 15:

‘Thus, an information infrastructure consists of a set of standards, protocols and gateways that link the running applications, programs and systems. It connects, supports and enables the exchanges of bits, data and information between different technological and human agents. A legal infrastructure is made by shared legal principles, rules and procedures that link the several national jurisdictions and help them communicate and inter-operate. In legal terms, this is mainly based on the EU principles of legal cooperation and mutual recognition. A more practical aspect is that legal objects (files, sentences, utterances) must keep their legal validity when they cross the borders of a jurisdiction. A semantic infrastructure provides mechanisms for inter-language communication, including human and automatic translators between different languages, in order to retain meaning. An institutional infrastructure consists of bureaucratic procedures and organisational routines that can carry out the relevant administrative and business processes across national borders’.

¹⁹⁰ eu-LISA, *Elaboration of a Future Architecture for Interoperable IT Systems at eu-LISA*, Tallin, 2019.

¹⁹¹ *Ibid.*, p. 11.

The IO Regulations¹⁹² largely consist¹⁹³ of dispositions regulating the so-called interoperability components, of which there are four:

- the ESP (European Search Portal);
- the sBMS (shared Biometric Matching Service);
- the CIR (Common Identity Repository), and
- the MID (Multiple-Identity Detector).

To these, the CRRS (Common Repository for Reports and Statistics) must be added. Although not labelled as a ‘component’, the CRRS is a new IT feature introduced by the IO Regulations that will integrate into the new architecture.

The IO Regulations spend a chapter on each component while the CRRS is dedicated a unique norm within the other ‘measures supporting interoperability’¹⁹⁴. The IO Regulations avoid speaking of technologies or technical means, but state purposes – i.e., they explain what a component does as opposed to how it works. Here, we must move to the analysis of how the interoperability components function in order to highlight their contribution in the management of personal data for borders, migration, and security purposes.

2.2.1. The European Search Portal (ESP)

The ESP is a unique interface that will enable the ‘fast, seamless, efficient, systematic and controlled access of Member States’ authorities and EU agencies to large-scale IT systems, interoperability components (the CIR and the MID¹⁹⁵), the Europol data¹⁹⁶, and to the Interpol databases¹⁹⁷ in accordance with competent authorities’ access rights set forth in the relevant

¹⁹² See Article 1 of the IO Regulations.

¹⁹³ Additional elements are directed at regulating data protection rights, responsibilities of the EU agencies and the Member States, the amendments brought to the legislative instruments affected by interoperability, and the final provisions.

¹⁹⁴ See eu-LISA, *Elaboration of a Future Architecture for Interoperable IT Systems at eu-LISA*, Tallin, 2019.

¹⁹⁵ See the analysis on Articles 20, 21 and 22 of the IO Regulations *infra*.

¹⁹⁶ Europol must develop the Querying Europol System (QUEST) interface for basic protection level to connect with the ESP and the CIR, and to enable searches within Europol’s information – see Article 57(1) of Regulation (EU) 2019/818. The purpose is to allow Europol to consult and retrieve the data stored in the CIR according to its mandate. In the European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, it was proposed that ‘a flagging mechanism should be set up at the CIR level to ensure that EUROPOL can only read/retrieve permitted identity data’, p. 53.

¹⁹⁷ Article 6(1) of the IO Regulations. In the case of Interpol, the IO Regulations clarify that: ‘[...] when querying the Interpol databases, the data used by an ESP user to launch a query is not shared with the owners of Interpol data. The design of the ESP should also ensure that the Interpol databases are only queried in accordance with applicable Union and national law’ – see recital (14) of the IO Regulations.

instruments'¹⁹⁸. In addition, the ESP will carry the queries of the Central Systems of the EES, the VIS, the ETIAS, the Eurodac, the SIS, the ECRIS-TCN, the CIR and the MID. Its usage will be mandatory, except for the cases concerning the SIS, Europol data¹⁹⁹, or the Interpol databases²⁰⁰, which suggests that the ESP will not be separated from the CIR as the Member States initially proposed, but will constitute the first search entry point for users or systems²⁰¹. However, Article 63 of the IO Regulations establishes a transitional period in which the usage of the ESP is not mandatory. According to this Article:

‘1. For a period of two years from the date the ESP commences operations, the obligations referred to in Article 7(2) and (4) shall not apply and the utilisation of the ESP shall be optional.

2. The Commission is empowered to adopt a delegated act in accordance with Article 69 in order to amend this Regulation by extending the period referred to in paragraph 1 of this Article once, by no longer than one year, when an assessment of the implementation of the ESP has shown that such an extension is necessary, especially in view of the impact that bringing the ESP into operation would have on the organisation and length of border checks’.

The ESP transitional period lasts two years – approximately from 1 January 2023 until 31 December 2024 – and is extendable for one year. It will enable the Member States to progressively use the ESP and, consequently, to ‘migrate’ the EU large-scale IT systems to the interoperability infrastructure. This implies that during such a period three main scenarios are foreseeable regarding accessing the data stored in the systems and the CIR:

- first, through the ESP;
- second, through the fallback procedure, and
- third, using the rights granting during the ‘transitional access’ phase.

Although the ESP is deemed to substitute bilateral connecting channels between the Central Systems and the National ones, a fallback procedure enabling direct access to the systems or the CIR has been maintained in case it is technically impossible to use the ESP, which means that the ICDs allow direct access to both the systems and the CIR²⁰². If a technical issue

¹⁹⁸ Article 71(1) of Regulation (EU) 2019/817 and Article 67(1) of Regulation (EU) 2019/818 establish that the national authorities using or accessing the ESP are notified to eu-LISA that must publish – and update – a list on the *OJ* three months from the date on which each interoperability component commenced operations. The European Commission, then, is in charge of notifying the Member States and the public through the website.

¹⁹⁹ The ESP will: on the one hand, enable competent authorities entitled to access the Europol data to consult it at the same time of another IT system; on the other hand, Europol staff could (optionally) consult the IT systems, including the SIS, and the Europol data through the ESP.

²⁰⁰ Recital (17) of the IO Regulations: ‘The ESP should also be used by Union agencies to query Central SIS in accordance with their access rights and in order to perform their tasks. The ESP should be an additional means to query Central SIS, Europol data and the Interpol databases, complementing the existing dedicated interfaces’.

²⁰¹ See the European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 43 ff. However, data will continue to be uploaded directly to the IT systems while the ESP will be used only for searching within them and the interoperability components.

²⁰² Article 11 of the IO Regulations.

concerns a failure of the ESP, the ESP users shall be notified in an automated manner by eu-LISA. If it is related to the national infrastructure in a Member State or an EU agency, then that Member State or EU agency shall notify eu-LISA and the European Commission in an automated manner. As we will further analyse below, the possibility to depict a third type of transnational access turns out to be a superfluous and expensive option that should be discarded by the Member States during the implementation stage.

From an architectural perspective, the ESP is a set of application programming interfaces that includes a search mechanism connected to the interfaces of the Member States' Interfaces of National Systems (NUI). Technically speaking, the ESP is made of three main elements:

- a central infrastructure, including a search portal enabling the simultaneous querying of the EES, VIS, ETIAS, Eurodac, SIS, and ECRIS-TCN as well as the Europol data and Interpol databases;
- a secure communication channel between the ESP, the Member States and the EU agencies that are entitled to use the ESP, and
- a secure communication infrastructure between the ESP and the EES, the VIS, the ETIAS, the Eurodac, the Central SIS, the ECRIS-TCN, the Europol data and the Interpol databases, as well as one between the ESP and the central infrastructures of the CIR and the MID.

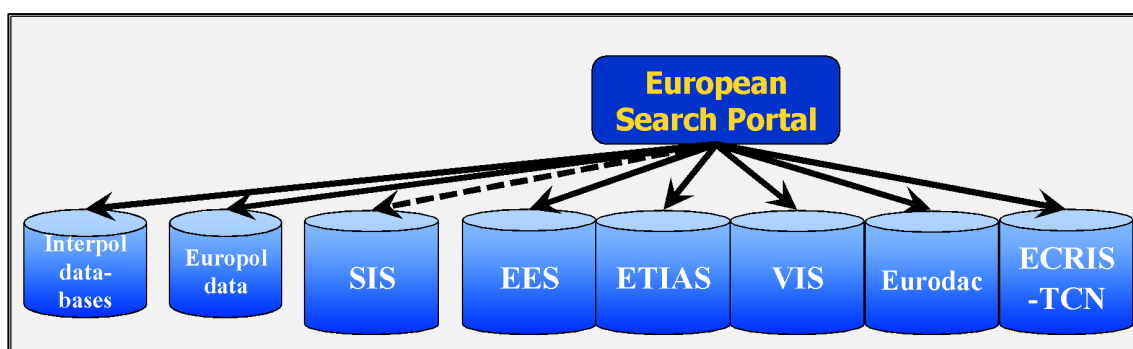


Figure 3 The European Search Portal (ESP) – Source: Commission Staff Working Document impact assessment, SWD(2017) 473 final, Strasbourg, 12.12.2017.

In practical terms, the ESP will enable its users – whether human or not – to launch queries to the systems' central infrastructures through the NUI interface²⁰³. The ESP acts as a one-stop shop or 'message broker', seamlessly retrieving the data held in the systems, the interoperability components, the Europol data, or the Interpol's databases while indicating where the data comes

²⁰³ The European Commission must adopt an implementing act specifying the technical procedure for the ESP – see Article 9(7) of the IO Regulations –, but it was not published when we closed our research.

from²⁰⁴. Its functioning can be compared to how search engines available on the web gather information stored in different sites on the basis of keyword research – e.g., Trivago²⁰⁵. Requests may be launched via biographical data²⁰⁶ – i.e, identity data and travel document data²⁰⁷, biometric data²⁰⁸, and so-called “business data”, that is data that is not stored in any interoperability component, but in the underlying large-scale IT systems, in the Europol data or in the Interpol’s databases. Provided that some business data can be shared among the underlying large-scale IT systems, the Europol data, or the Interpol databases – e.g., the visa sticker number that is known both to the EES and the VIS – this can be used to query systems through the ESP at the same time.

The ESP will be used by numerous Member States’ authorities and EU agencies that have access to at least one of the underlying IT systems or interoperability components. These authorities, Union agencies and systems are the users of the ESP which are to be laid down in the European Commission’s implementing decisions on ESP queries and replies²⁰⁹ which lays down the technical details for the ESP user profiles. The ESP user profile indicates the Member State or the EU body to which the competent authority or staff person querying the systems belongs – e.g., the Spanish border guard – and comprises²¹⁰:

- the fields of data to be used for a query;
- the EU information systems, the Europol data, and the Interpol databases that are to be queried, those that can be queried, and those that are to provide a reply to the user;
- the specific data in the EU information systems, the Europol data and the Interpol databases that may be queried, and
- the categories of data that may be provided in each reply²¹¹.

²⁰⁴ Opinion of the EDPS No. 4/2018 on the *Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, Brussels, 18.04.2018, p. 8.

²⁰⁵ Available at www.trivago.com.

²⁰⁶ “Biographical data” includes both identity data and travel document data, yet we will try to use the least this concept to avoid misunderstandings.

²⁰⁷ Article 9(2) of the IO Regulations. To be noted that Article 4(13) set forth that ‘travel document’ means ‘a passport or other equivalent document entitling the holder to cross the external borders and to which a visa can be affixed’ which seems to exclude national identity cards enabling the crossing of external borders for EU citizens. If so, this would result in an important shortcoming to combat identity frauds in case of EU citizens’ lost and stolen identity documents.

²⁰⁸ Article 9(1) of the IO Regulations.

²⁰⁹ The implementing decision has not been published yet, but the EDPS has already issued its comment. In it, it urged the European Commission to make reference to these systems in the definition of “users” provided for the implementing decision. See the Formal comments of the EDPS on the *draft Commission Implementing Decisions specifying the technical procedure for the European search portal to query the EU information systems, Europol data and Interpol databases and the format of the European search portal’s replies, pursuant to Article 9(7) of Regulation (EU) 2019/817 of the European Parliament and of the Council*, Brussels, 17.05.2021.

²¹⁰ Article 8(1) of the IO Regulations.

²¹¹ The ESP users’ profiles must be defined by the European Commission by an implementing act with the cooperation of eu-LISA and the Member States – confront Article 8(2) of the IO Regulations. Under this decision,

Once the ESP user has launched a query, this is split into distinct queries for each information system that is being queried, though the querying occurs simultaneously according to the ESP user profile access rights. Each information system, or interoperability component, queried shall return a reply via the web service-based interface of that system using a data format based on common standards. The replies are provided separately as soon as the underlying system or component replies. The system's reply indicates:

- whether one or more sets of data stored in a queried IT system can fulfil the search criteria, and
- if that data has been found, in which case the ESP must:
 - specify the type of match, and
 - provide a reference to the data stored in the queried IT system.

If no data stored in the system queried fulfils the search criteria, the reply will indicate that there is no match. It is also possible that the queried system experiences an error, in which case, the system's reply will specify the type of error that occurred. The ESP shall provide each individual reply from the information systems queried, and these must be separated according to the information system that returns each reply. A reply shall be considered 'complete' when it includes the results from all the information systems queried by the ESP, indicating whether the data has been found or not. Conversely, when at least one system, the CIR, or the MID, does not return a reply, the reply is considered incomplete. Besides, if a queried system does not reply within the time specified for that system, the ESP shall indicate it in its reply to the ESP user. However, and unlike the sBMS analysed below, the timeout thresholds by which the systems must reply have not been harmonised through interoperability, but rather are defined by each IT system.

2.2.2. The shared Biometric Matching Service (sBMS)

All systems storing biometric data allow for the identification of individuals, being it through a verification or an identification process – i.e., with an AFIS or an ABIS²¹². The sBMS²¹³ is a container of biometric templates²¹⁴ representing the correspondent biometric data stored in the

each user is assigned a profile – i.e., a code – depending on the purposes of the queries. They are revised on a year basis by eu-LISA together with the Member States and, if needed, they are updated.

²¹² See Els Kindt and Lorenz Müller, *loc. cit.*

²¹³ See eu-LISA *Feasibility Study – final report*, Tallin, 2018, available at ww.eulisa.europa.eu.

²¹⁴ See Article 13(1) of the IO Regulations. It is not clear whether biometric templates constitute or not personal data – i.e., whether they enable or not the (in)direct identification of an individual.

different IT systems and in the CIR²¹⁵ – as a result, it does not store any ETIAS templates as this system does not process biometrics – this will be implemented together with the EES. Although storing less information than raw biometric data, templates provide for the unique identification of individuals and, as such, it is preferable to still consider them as sensitive data²¹⁶. Technically, the sBMS is made of:

- a central infrastructure, which will replace the central systems of the EES, VIS, SIS, Eurodac and ECRIS-TCN respectively, to the extent that it shall store biometric templates and allow searches with biometric data, and
- a secure communication infrastructure between the sBMS, the C-SIS, and the CIR enabling the data stored in the CIR to directly communicate with the sBMS.

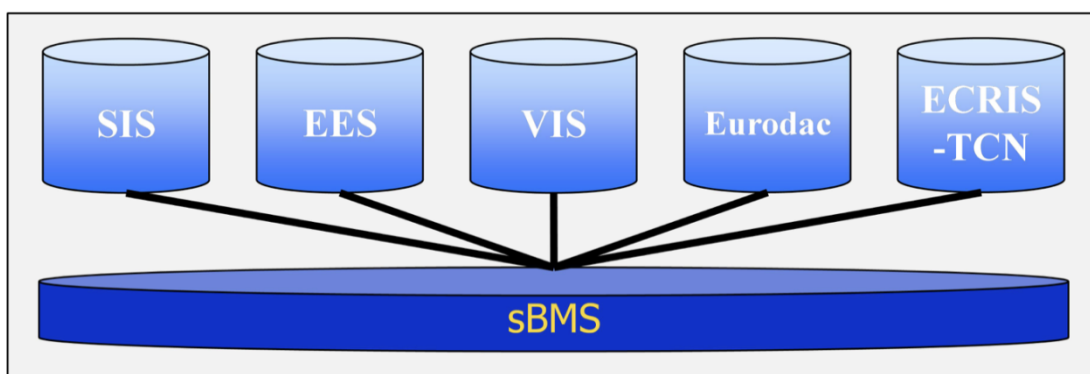


Figure 4 shared Biometric Matching Service (sBMS) - Source: Commission Staff Working Document Impact Assessment, SWD(2017) 473 final, Strasbourg, 12.12.2017.

Before accessing the templates in the sBMS, the correspondent data is submitted to an automated data quality check²¹⁷ performed by the sBMS itself. This check is in addition to the data quality tests already existing for all large-scale IT systems²¹⁸ and must be seen as important, as the higher the quality of data, the lower the risk of false positives and negatives. The templates stored in the sBMS are kept separate according to the EU system in which the

²¹⁵ Note that in the European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, the European Commission advanced the possibility to merge the sBMS with the CIR and, actually, it presented this option as the most efficient one. The HLEG on information systems and interoperability, *Final Report*, Ares(2017)2412067, Brussels, 11.05.2017, p. 36, instead, advanced the possibility to merge in it Europol's biometric data too. During the implementation phase, the possibility to merge Europol's biometrics templates into the sBMS was re-proposed to eu-LISA and the European Commission, which would require the corresponding amendment in the IO Regulations. However, the European Commission was reluctant on this point.

²¹⁶ See the Opinion of the Article 29 DPWP on *Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration*, Brussels, 11.04.2018, p. 8.

²¹⁷ Article 37(2) of the IO Regulations.

²¹⁸ Article 13(3) of the IO Regulations. The European Commission is called on to adopt an implementing decision on the sBMS performance specifying the proceeding to monitor the performance of the sBMS especially in case for ensure the feasibility of biometric searches in time-critical procedures – e.g., for border checks and identifications, see Article 13(5) of the IO Regulations.

corresponding biometric data is stored and a reference to the sBMS records is stored in the relevant IT system²¹⁹. The sBMS can perform comparison processes among the templates stored in it and with the data sample captured live. The result is a score that evaluates the similarities among the templates or between the template and the matched sample. In sum, the sBMS is equipped with a decision function that decides if the biometric template/sample matches a certain reference template, or not. Once the correspondent biometric data is erased, then, the biometric template shall also be deleted in an automated manner²²⁰.



Figure 5 Biometric sample and template – Source: www.shutterstock.com.

In terms of system performance – i.e., its speed of operation – the sBMS is expected to perform nine operational services according to predefined targets, that include:

- the biometric verification – or one-to-one matching – of facial images and fingerprints²²¹;

²¹⁹ Article 13(2) of the IO Regulations.

²²⁰ Article 15 of the IO Regulations.

²²¹ We recall that biometric verification – also known as authentication or one-to-one search – allows the verification that the data subject is who s/he claims to be. It consists in the comparison between the biometric samples and the biometric template previously recorded in a physical or electronic medium, such it is for example the matching of a live template with the sample stored in the chip of a visa or a passport – ISO/IEC 2382-37:2017(en) Information technology — Vocabulary — Part 37: Biometrics, para. 3.8.3, and Terri Givens, Gary P. Freeman, and David L. Leal, *Immigration Policy and Security*, New York, Routledge, 2008. Biometrics were firstly inserted in EU passports and travel documents with Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, *OJ L* 385, 29.12.2004, pp. 1-6, in order to accomplish with the US Visa Waiver Program – see the Opinion of the Article DPWP No. 3/2005 on *Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member State*, Brussels, 30.09.2005. They were subsequently inserted in EU visas – Regulation (EC) No 390/2009 of the European Parliament and of the Council of 23 April 2009 amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications, *OJ L* 131, 28.5.2009, pp. 1-10 –, and residence permits – Council Regulation (EC) No 380/2008 of 18 April 2008 amending Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals, *OJ L* 115, 29.4.2008, pp. 1-7. In this sense, biometrics enable to check the validity of the travel document as the CJEU validated in *C-291/12, Michael Schwarz v Stadt Bochum*, 17 October 2013, EU:C:2013:670.

- the biometric identification – or one-to-many matching – by multi-modal data, fingerprints and facial image²²²;
- the insertion, update, and deletion of biometric data, and
- a check on the quality of the biometrics.

Thus, its response may consist in: an error message, an acknowledgement message, a quality control transaction, or a search result.

The performance of the sBMS is monitored by eu-LISA that is firstly in charge of evaluating whether the same accuracy values²²³ set forth for the verification and identification of each EU information system's legislative text need to apply three years after it begins operation. If new values are to be defined, it is up to eu-LISA to lay them down with the assistance of the European Commission, the Member States, and other Union agencies. As the EDPS²²⁴, the European Commission Implementing Decision on the sBMS performance – that has not yet been published – does not define how this cooperation would take form, though we can assume that existing groups, such as the eu-LISA Advisory Group on interoperability, might be chosen. According to the EDPS, even more worrisome is the fact that eu-LISA's empowerment with respect to reviewing the accuracy values may result in a delegation of discretionary activities unless the European Commission ultimately be in charge of assessing and approving the values proposed by the Agency. Thus, the EDPS suggested that the European Commission align its implementing decision accordingly.

In its monitoring function, eu-LISA must ensure the effectiveness of the sBMS which is understood to have the shortest response time, even in critical cases. As a result, Member States

²²² We recall that biometric identification consists in the crossmatching of the biometric samples of a person with all biometric references that are recorded in a database – ISO/IEC 2382-37:2017(en) Information technology — Vocabulary — Part 37: Biometrics, para. 3.8.2. This responds, for example, to the need of locating a person on a list of individuals under supervision – in other words, a watch list. Thus, while verification has been used so far to find out identity thefts and frauds, identification is a technique aimed at tracking down suspects and criminals – see the High Court of Justice, *The Queen (on application of Edward Bridges) - and - the Chief Constable of South Wales Police*, 4 September 2019, CO/4085/2018, available at www.judiciary.uk, in favor of the necessity and proportionality of the South Wales Police PrOject in Cardiff for the processing and comparison of digital images of pedestrians by means of surveillance cameras with those stored in lists of persons previously registered. From a data protection perspective, biometric identification is more intrusive than verification since it requires the simultaneous comparison of personal data with an indefinite number of templates previously stored in a database – confront the Working document of the Article 29 DPWP on *biometrics*, Brussels, 1.08.2003, p. 6. Moreover, and despite its utility, biometric identification pushes for the massive storage of personal data which triggers the delicate issue of cyber surveillance that we analysed in Chapter I.

²²³ The accuracy of biometric data is set forth in the European Commission implementing act on common data quality indicators and the minimum quality standards for storage of data that will be analysed in due course. Volume performance, instead, is not laid down neither in the IO Regulations, nor in the European Commission secondary legislation.

²²⁴ See the Formal comments of the EDPS on *the Commission Implementing Decisions laying down the performance requirements and practical arrangements for monitoring the performance of the shared Biometric Matching Service pursuant to Regulation (EU) 2019/817 and Regulation (EU) 2019/818 of the European Parliament and of the Council*, Brussels, 31.03.2021.

must designate and train personnel in charge of communicating, reporting, and answering to eu-LISA in relation to the operations of the sBMS. As part of its monitoring process, eu-LISA is expected to assess the sBMS's performance by elaborating business use cases²²⁵. If the sBMS does not comply with performance standards, eu-LISA should be alerted, though its responsibility is limited to ensuring the performance and operations response requirements that fall within its control.

2.2.3. The Common Identity Repository (CIR)

The CIR²²⁶ is a piece of front-end infrastructure²²⁷ that stores the personal data held by the underlying systems, in accordance with their logical separation²²⁸, with the sole exception of the SIS, where the merging of data into the CIR²²⁹ was excluded for technical reasons²³⁰ and, also, due to political concerns, as it is the only system storing EU citizens' personal data. Technically speaking, the CIR is made up of²³¹:

²²⁵ In the business use cases eu-LISA studies practical examples deriving from the application of the large-scale IT systems and the interoperability components to real-life.

²²⁶ See the European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017.

²²⁷ *Ibid.*, p. 39:

‘If set up as a front-end component, connection to the CIR would be invoked directly by end-users via a national system(NS). An end-user would send an identity search request to the CIR, which would then process the request (i.e. detect if there is an occurrence of multiple identities for the requested identity search) and then return results accordingly to the user. How the CIR would be populated or if it would invoke other components in the background would be seamless to the user’.

²²⁸ During the so-called ‘transitional period’ the CIR will be fed with the data processed in each of the different IT systems whose historical data will migrate into the CIR. Later on, the competent authorities will directly store the biographic data therein. Although decentralised databases might be connected with the interoperability architecture, they are not part of the CIR; these decentralised databases are: the Europol data and the Interpol databases whose data will be cross-checked with the data stored in the CIR through the ESP.

²²⁹ ‘The complex technical architecture of SIS containing national copies, partial national copies and possible national biometric matching systems would make the CIR very complex, and changes to the 30 (non-standardised) national copies would be excessively expensive to a degree where it may no longer be feasible’, according to the Commission Staff Working Document impact assessment, SWD(2017) 0473 final, Strasbourg, 12.12.2017. See also Marco Velicogna, “The Making of Pan-European Infrastructure: From the Schengen Information System to the European Arrest Warrant”, in Francesco Contini and Giovan Francesco Lanzara, *op. cit.*, pp. 185-215. The European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 3, refers to the MID as a Common Identity Linker and finds that its separation from the CIR was the better solution in terms of security requirements needed to access the SIS. The Common Identity Linker should have been a linkage broker managing the interaction between the SIS and the CIR: ‘The common identity repository in option 2 would become extremely complex and expensive when extracting the biographic data from SIS and migrating this to the CIR. To provide an alternative to not including SIS data in the CIR and not being able to link SIS data with biographical data of third-country nationals, a new component would be necessary’.

²³⁰ Commission Staff Working Document impact assessment, SWD(2017) 0473 final, Strasbourg, 12.12.2017: ‘The common identity repository in option 2 would become extremely complex and expensive when extracting the biographic data from SIS and migrating this to the CIR. To provide an alternative to not including SIS data in the CIR and not being able to link SIS data with biographical data of third-country nationals, a new component would be necessary’.

²³¹ Article 17(2) of the IO Regulations.

- a central infrastructure that replaces the central systems of the EES, the VIS, the ETIAS, the Eurodac and the ECRIS-TCN respectively, to the extent that it stores the data referred to in Article 18 of the IO Regulations;
- a secure communication channel between the CIR, Member States, and the Union agencies that are entitled to use the CIR in accordance with Union and national law, and
- a secure communication infrastructure between the CIR and the EES, the VIS, the ETIAS, the Eurodac and the ECRIS-TCN, as well as with the central infrastructures of the ESP, the sBMS and the MID.

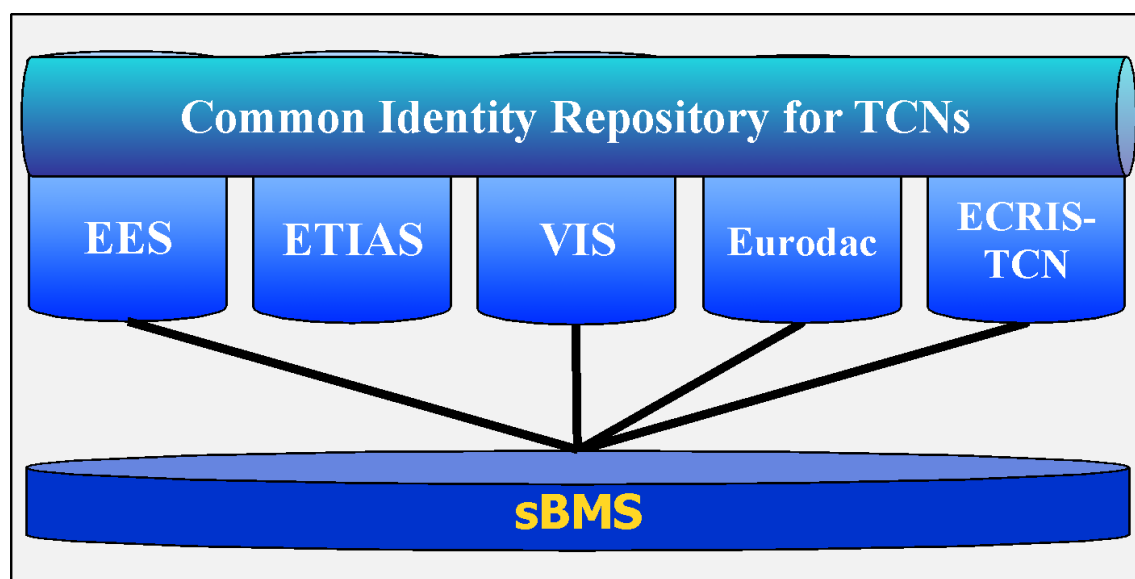


Figure 6 The Common Identity Repository – Source: Commission Staff Working Document impact assessment, SWD(2017) 473 final, Strasbourg, 12.12.2017.

Although the CIR has been assimilated to form a ‘monster database’²³², capable of storing the information of some 242 million identity records on third-country nationals²³³, not all data stored in the five large-scale IT systems in question are stored in the CIR²³⁴, rather, it is made up of the following categories²³⁵:

²³² Chris Burt, “EU Parliament approved unified biometric and bio database of 350 million people”, *BIOMETRICUPDATE.COM*, 4.22.2019, available at www.biometricupdate.com. We believe that the concept of “database” may not suit the interoperability components if it is taken into account that no new data is stored therein. The sole exception is made by the MID since – as analysed below – it will store the links generated and established among the individual files stored in the CIR.

²³³ European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 2.

²³⁴ The conclusions of Pika Šarf, *op. cit.*, p. 98, are therefore not correct.

²³⁵ The European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 28 ff., advanced different combinations of data that could have been stored in the CIR: first, the links stemming from matched data and the decisions made by a user about a link; second, core identity data – i.e., biographical data – together with links/decisions data and, third, extended identity data – i.e., biographical and travel document data

- raw biometric data²³⁶;
- travel document data²³⁷, and
- identity data²³⁸.

As with the sBMS, the data is subjected to a quality check before its insertion into the CIR, according to Article 18(4) of the IO Regulations. Notably, the CIR itself will improve the accuracy of the data stored therein by, for example, detecting typos, inversions in dates, or transliteration errors as we will further analyse in light of the objective pursued by the interoperability Article 21²³⁹. The CIR will be developed together with the implementation of the EES' common repository for biometrics and alphanumeric data and expanded with the implementation of the ETIAS²⁴⁰, while the data held in the other systems is expected to progressively "migrate" to the CIR²⁴¹. From the Feasibility Study on a Common Identity Repository (CIR) conducted by the European Commission in 2017, we note that the CIR might have been deployed in one of the two following ways:

- an identity analysis solution containing different categories of personal data from the underlying IT systems and generating links among the identifiers stored therein, or
- an identity repository tool designed to extract data from the underlying IT systems to centrally manage the identity information²⁴².

– with links/decisions data. The latter solution was found to provide the fullest support to border checks processes while giving support to other ones as it is the case of second-line checks or in case of visa applications.

²³⁶ Article 4(11) of the IO Regulations.

²³⁷ Article 4(13) of the IO Regulations.

²³⁸ See the European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 24, and Articles 4(8) and 27(3) of the IO Regulations. These are the data usually contained in a passport.

²³⁹ European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 54.

²⁴⁰ Article 18 of the IO Regulations.

²⁴¹ European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 96 ff. As the study explains, neither the EES nor the subsequent ETIAS' data have to 'migrate' to the CIR, but the VIS, Eurodac and ECRIS-TCN ones will have to be incorporated to it. The study highlights that the so-called 'legacy data' already stored in the systems may be de-duplicated at one, or new links can be progressively deployed through Member States' workflows – i.e., the legacy data would not migrate to the CIR until the multiple identity detection procedure linked them with the new data entered in one of the underlying IT systems and in the CIR. The co-legislators opted for the first option and to empowered the ETIAS Central Unit to resolve the links generated from the legacy data as we analyse *infra*.

²⁴² European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 4 and p. 38:

'Compared to an identity analysis tool, an identity repository would allow for centralised identity management as all data related to an identity would be stored in a same system. Such central management would be much more efficient and less error prone, as centralised identity information would always be up-to-date in each system and as management processes (including governance, security, etc.) would only need to be defined once. This would however require significant changes in the already existing central systems, as all identity-related data would have to be extracted to the repository. Furthermore, the business applications would need to be re-factored to be able to both connect to the repository for obtaining their data and to work with identity information that is managed externally and can thus be updated by other central systems'.

The co-legislators opted for a hybrid solution where the CIR results in a centralised identity management solution with limited impact on the existing large-scale IT systems as proposed by the European Commission²⁴³. Thus, the CIR has been equipped to perform three types of operation:

- first, it searches in a standardised, timely, and consistent manner all identity data stored in the CIR;
- second, it creates, updates, reads and deletes records in order to store and retrieve data, and
- third, it detects links within the identity data belonging to several systems²⁴⁴.

However, the co-legislators refused to copy the data from the systems to the CIR as proposed by the European Commission. In respect of the principle of data minimisation, the data will be stored in the CIR alone²⁴⁵. If any data is added to, amended, or deleted in one of the large-scale IT systems, it will be added, amended, or deleted in the CIR, too²⁴⁶. Moreover, the CIR stores personal data in a separated manner in order to respect its origin and keep a reference of the system/s and of the record from which the data originates²⁴⁷. Such a configuration represents another achievement of the interoperability architecture *vis-à-vis* the data protection by design and by default principles.

As we will analyse in detail below, as soon as a new white or red link is created by the MID in an automated manner, or established by the competent authority for manual verification, the CIR adds the new data – i.e., the links – to the existing file, while avoiding creating a new file²⁴⁸. Where a new white or red link is created or established later on²⁴⁹, the CIR adds this new data to the existing individual file. As a result, as far as they belong to the same person, the identity data lost in the underlying systems is gathered in an individual per-person file stored in the CIR. According to the European Commission, the concept of ‘identity’ resulting from the CIR consists of ‘[...] a collection of attributes that together are sufficient to uniquely identify

²⁴³ European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 97.

²⁴⁴ European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 53.

²⁴⁵ According to the *High-Level Expert Group on information systems and interoperability. Final Report*, Ares(2017) 2412067, Brussels, 11.05.2017, p. 34: ‘A view is an up-to-date snapshot of some of the original data. It neither copies nor allows modification of data. It is a perfect reflection of the original data. A view is like a pair of glasses, one can see different things depending on the type of lens’. A “virtual view” of the data stored in the CIR will be available in the underlying IT systems only for the time necessary to set in motion the interoperability components.

²⁴⁶ Articles 19 and 23 of the IO Regulations, specifying that: ‘The creation of a link shall not affect the retention period of each item of the linked data’.

²⁴⁷ Article 18(2) and (4) of the IO Regulations. In case of failure, it is the CIR itself that should warn eu-LISA in an automated manner of its technical unavailability.

²⁴⁸ Article 19(2) of the IO Regulations. On the MID see further below.

²⁴⁹ See further below.

an entity within a set of similar entities'²⁵⁰. In other words, the CIR is expected represent the first model for managing third countries nationals' identities at the EU level, as:

‘The deployment of the CIR would thus constitute the first step towards an optimised and person-centric environment in which all aspects of a person’s identity are fully managed centrally and separated from the core business of each European central system’²⁵¹.

This suggests that the CIR is not merely an identity management system consisting of ‘[...] the management of these attributes by various people who can create, modify, update or delete them when relevant’²⁵², but also a Schengen-based CMS ‘in which all aspects regarding the identity of a person would be managed centrally’²⁵³. Thus, the ‘correct identity’ the EU-legislator is looking for is ‘a new mode of ‘truth’ production in the form of a dedicated ‘identity confirmation file’ that is supposed to re-introduce a reliable baseline for the government of the Schengen area’²⁵⁴. If so, the need to centrally store personal data should have been justified separately in light of the principle of necessity and proportionality²⁵⁵ and, specifically, the co-legislators should have proven that the CIR contributes to a more effective application of freedom, security and justice objectives²⁵⁶. Provided that the CIR is used for different purposes that are differently regulated under the EU data protection *acquis*²⁵⁷, such an assessment should have been carried out accordingly²⁵⁸ while highlighting that no discrimination is made between

²⁵⁰ European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 23.

²⁵¹ *Ibid.*, p. 5.

²⁵² *Ibid.*, p. 11; according to Elena María Torroglosa García, *Digital Identity Management Through the Interoperability of Heterogeneous Authentication and Authorization Infrastructures*, Ph.D. dissertation, University of Murcia, 2017: ‘Identity Management Systems offer users tools and mechanisms to help them in the task of controlling credentials and personal information. These mechanisms range from the credential management and privacy assurance to Single Sign-On among others. From the point of view of Service Providers, Identity Management Systems allow the simplification of user management, since they assume the delegation of the authentication process and credential storage’, p. xi.

²⁵³ *Ibid.*, p. 14.

²⁵⁴ Matthias Leese, “Fixing State Vision: Interoperability, Biometrics, and Identity Management in the EU”, *Geopolitics*, 2020, pp. 1-21, p. 1.

²⁵⁵ Opinion of the Article 29 DPWP on *Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration*, Brussels, 11.04.2018, p. 6: ‘So far in the view of the WP29, the necessity of a consolidated database including biometric identifiers has not been established yet and the mere fact that some databases containing these types of data have already been created and constitute precedents does not demonstrate this necessity. In any case, assuming the necessity could be sufficiently established, considerable concerns would still remain regarding the proportionality of the proposal. What is created here is in sum a database including a huge number of TCN being present in the EU (as well as TCN willing to come and TCN having already left)’.

²⁵⁶ C-524/06, *Heinz Huber v Bundesrepublik Deutschland*, 16 December 2008, ECLI:EU:C:2008:724, concerning Mr. Heinz Huber’s request to delete his personal data from the German Central Register of Foreign Nationals on the basis of the principle of non-discrimination since, differently from other EU citizens, German nationals did not have their data centrally stored.

²⁵⁷ See *infra*.

²⁵⁸ C-524/06, *Heinz Huber v Bundesrepublik Deutschland*, para. 46:

‘Consequently, the compatibility with Community law of the processing of personal data undertaken through a register such as the AZR should be examined, first, in the context of its function of providing support to the authorities responsible for the application of the legislation relating to the right of residence and to its use for

third-country nationals and EU citizens²⁵⁹. We should not forget that, as far as Union citizens are concerned, in May 2021 the European Commission proposed the establishment of a European Digital Identity Wallets based on the biometric authentication of individuals²⁶⁰, which excludes centralised data storage.

2.2.4. The Multiple-Identity Detector (MID)

The MID may be defined as a “complementary database” in charge of creating, establishing, and storing the links among personal data stored in the CIR and the SIS, for which purpose it acts through the ESP and the sBMS. The MID was added as a result of a recommendation following the European Commission’s impact assessment because of the impossibility to “migrate” the SIS into the CIR, which leads us to hypothesise that if the SIS could have been merged within the CIR, the latter could have stored the links²⁶¹. However, it is also true that the SIS is the sole system containing personal data on EU citizens – being that the ECRIS-TCN is processing the data of dual EU-third country nationals – so that its centralised storage could be contrary to the principles of subsidiarity and proportionality. Whatever the explanation, the solution found by the co-legislators – i.e., the placing the MID outside the CIR – must be welcomed from a privacy by design and privacy by default perspective, as it avoids concentrating linked-personal data in the CIR²⁶².

The MID is made up of:

statistical purposes, by having regard to Directive 95/46 and more particularly, in view of the third question, to the condition of necessity laid down by Article 7(e) of that directive, as interpreted in the light of the requirements of the Treaty including in particular the prohibition of any discrimination on grounds of nationality under Article 12(1) EC, and, secondly, in the context of its function in the fight against crime, by having regard to primary Community law’.

²⁵⁹ *Ibid.*, para. 80, where the CJEU sentenced that for the purposes of fighting crime EU citizens and German nationals must be equally treated since their persecution is carried out irrespective of the nationality of the perpetrators. Conversely, the CJEU noted (paras. 47-68) that the Council Directive 68/360/EEC of 15 October 1968 on the abolition of restrictions on movement and residence within the Community for workers of Member States and their families, *OJ L 257*, 19.10.1968, pp. 13-16, allows Member States to ask for certain formalities to be satisfied in order to regularly reside in another Member State for a more than three-months period, notwithstanding the fact that the proportionality of the central storage of personal data must be further assessed.

²⁶⁰ See the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM(2021) 281 final, Brussels, 3.6.2021, and Paloma Llaneza González, *Identidad digital*, Madrid, Wolters Kluwer, 2021, p. 67 ff.

²⁶¹ According to the Proposal for a Regulation of the European Parliament and of the Council, COM(2017) 0794 final, Brussels, 13.12.2017, p. 19: ‘The fourth interoperability component proposed in this draft Regulation (the multiple-identity detector) was not identified by the high-level expert group, but arose during the course of additional technical analysis and the proportionality assessment conducted by the Commission’.

²⁶² European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 1: ‘One solution proposed and further examined in this report is a Common Identity Repository (CIR) that could act as a single component centralising the search of identity data for third country nationals (TCN) and storing the connections (links) between all the identities for TCNs that appear in more than one of the EU central systems’. The study reports that ‘the CIR should put in place a physical separation of the identity data owned by the SIS’ to respect the privacy by design principle (p. 48).

- a central infrastructure, storing links and references to EU information systems, and
- a secure communication infrastructure to connect the MID with the SIS and the central infrastructures of the ESP and the CIR.

It is therefore connected with the SIS, the CIR, and the ESP. The MID contains an identity confirmation file that gathers:

- the links referred to in Articles 30 to 33 of the IO Regulations – i.e., red, green, and white links;
- an alphanumeric code of reference to the EU information systems in which the linked data is held;
- an alphanumeric code of a single identification number allowing the retrieval of the linked data from the corresponding EU information systems;
- an alphanumeric code of reference for the authority responsible for the manual verification of different identities, and
- the date of creation, or update, of the link.

The possibility to save the links established among the identity files – or identity groups in eu-LISA's jargon – i.e., the identity data, travel document data, and biometrics belonging to the same person, but stored across the large-scale IT systems, allows users to see the prior identity checks carried out on the individual. Consequently, only in cases where the circumstances surrounding a specific individual change – because they change their personal data and/or they are newly registered in another large-scale IT system – then, the existing links are updated or a new one/s are created²⁶³. The identity confirmation file and the data stored therein, including the links, is stored in the MID only as long as the linked data is stored in two or more EU information systems. Afterwards, it must be erased from the MID in an automated manner.

Article 69 of the IO Regulations establishes a transitional period for the MID in the following terms:

‘For a period of one year following notification by eu-LISA of the completion of the test of the MID referred to in Article 72(4)(b) and before the start of operations of the MID, the ETIAS Central Unit shall be responsible for carrying out multiple-identity detection using the data stored in the EES, VIS, Eurodac and SIS. The multiple-identity detections shall be carried out using only biometric data’.

The MID's transitional period lasts one year – and it is expected to last from 1 January 2023 until 31 December 2023 – extendable by a three-to-six month period and provides for the ETIAS Central Unit – and the SIRENE Bureau as far as the SIS's sensitive alerts are concerned – the ability to resolve the MID's yellow links. What we intend regarding the resolution of

²⁶³ See below the analysis on the access to the CIR for the detection of multiple identities.

yellow links will be addressed in due course. Here, it suffices to say that the MID's transitional period will overlap with that of the ESP, which raises the question of whether Member States will be able to use the MID before "migrating" to the ESP. Such "transitional access" to the MID requires eu-LISA to implement an additional tool – i.e., a specific ICD – enabling the triggering of the multiple-identity detection procedure in case an individual file is inserted or updated in one of the underlying systems – see *infra*. This option would become in practice overly complicated without the ESP²⁶⁴ so that during the implementation of the IO Regulations, eu-LISA made it clear that the ESP should be "partially" implemented, at least to support the MID procedure.

2.3. Interoperability's own objectives

Article 2(1) of the IO Regulations establishes the objectives pursued by the sister Regulations that come close to coinciding with the purposes deriving from the underlying large-scale IT systems. These objectives are:

- to improve the effectiveness and efficiency of border checks at external borders;
- to contribute to the prevention and the combating of illegal immigration;
- to contribute to a high level of security within the AFSJ of the Union, including the maintenance of public security and public policy and safeguarding security in the territories of the Member States;
- to improve the implementation of the common visa policy;
- to assist in the examination of applications for international protection;
- to contribute to the prevention, detection and investigation of terrorist offences and of other serious criminal offences, and
- to facilitate the identification of unknown persons who are unable to identify themselves or unidentified human remains in case of a natural disaster, accident or terrorist attack.

Article 2(2) of the IO Regulations foresees that the interoperability objectives listed in its paragraph (1) must be achieved through a series of functions that, from our perspective, can be systematised as follow:

- first, interoperability is called on to support the purposes of the underlying large-scale IT systems by facilitating the access to information by border guards, law

²⁶⁴ Specifically, it requires the implementation of an additional ICD enabling Member States not to implement the ESP while using the MID.

enforcement officers, immigration officials, and judicial authorities ‘while ensuring necessary and proportionate conditions for that access’, and

- second, interoperability provides for the implementation of the so-called interoperability components which aim at:
 - ensuring the correct identification of persons (Article 20);
 - contributing to combating identity fraud (Article 21), and
 - streamlining the conditions for the designated authorities’ access to the IT systems, while ensuring necessary and proportionate conditions for that access (Article 22).

Interoperability’s supporting function aside – which we addressed above while analysing the new IT architecture that incorporates the EU systems – the specific purposes pursued by interoperability can be found in Articles 20, 21 and 22 of the sister Regulations. These Articles introduce new objectives to those already pursued by the underlying IT systems and are achieved by accessing the CIR²⁶⁵.

Finally, Article 2(2)(c) and (e) specify that the IO Regulations:

- improve data quality and harmonise the quality requirements for the data stored in the EU information systems while respecting the data processing requirements of the legal instruments governing the individual systems, data protection standards and principles, and
- strengthen, simplify, and make more uniform the data security and protection conditions that govern the respective EU information systems, without affecting the special protection and safeguards afforded to certain categories of data.

Data quality and data security measures are delegated to eu-LISA’s expertise²⁶⁶, but do not add new objectives to the underlying large-scale IT systems that, in reality, already include their own relevant provisions. Therefore, these topics will be analysed after having examined the *quid 413luris* brought by the sister Regulations to (the already multi-purpose) large-scale IT systems.

²⁶⁵ In the end, the CIR will store the individual files of each person registered in the underlined systems and speed up the retrieval of such data through the queries launched by the ESP users.

²⁶⁶ Which includes the following ancillary objectives: improving data quality and harmonising the quality requirements for the data stored in the EU information systems (Article 2(2)(c) IO Regulations) while respecting the data processing requirements of the legal instruments governing the individual systems, data protection standards and principles; facilitating and supporting technical and operational implementation by Member States of EU information systems (Article 2(2)(d) IO Regulations), and strengthening, simplifying and making more uniform the data security and data protection conditions that govern the respective EU information systems, without affecting the special protection and safeguards afforded to certain categories of data (Article 2(2)(e) IO Regulations).

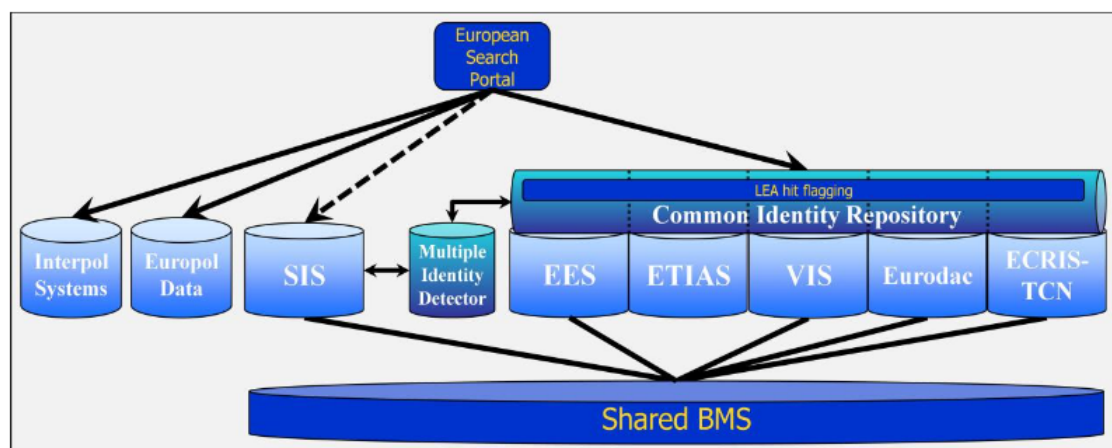


Figure 7 The whole picture – Source: Commission Staff Working Document impact assessment, SWD(2017) 473 final, Strasbourg, 12.12.2017.

2.3.1. The access to the CIR for identification purposes: The purpose of Article 20

According to the European Commission, before the IO Regulations were proposed, only the C-SIS could be consulted by police authorities in order to verify an individual’s identity within the territories of the Member States²⁶⁷. The so-called databases on migration, could not have been checked as they were primary directed at resolving issues surrounding the management of migratory flows and their querying by law enforcement purposes to fight terrorist or other serious criminal offences was an “ancillary” use²⁶⁸. Therefore, the Convention implementing the Schengen Agreement could not regulate checks at either the internal borders or within the Member States’ territories²⁶⁹.

With Article 20 of the IO Regulations, the EU manages to expand the scope of large-scale IT systems for the purpose of identification in terms of the so-called one-to-many search, that is, the possibility of tracking down a person due to their biometric data having already been registered in a database²⁷⁰. In principle, Article 20 is not concerned with one-to-one

²⁶⁷ Article 27 of Regulation (EC) No 1987/2006.

²⁶⁸ Commission Staff Working Document impact assessment, SWD(2017)0473 final, Strasbourg, 12.12.2017, para. 2.3.:

‘In other situations that are not related to migration management or to terrorism and other serious crimes, e.g. the prevention, detection or investigation of crimes that do not pass the threshold of ‘serious’, or when helping victims of accidents or crime, the police officer is not authorised to access Eurodac, VIS or the future EES to identify a third-country national on the territory. This impedes authorities in detecting multiple identities and identity fraud’.

²⁶⁹ *Ibidem*.

²⁷⁰ Some reflections on Article 20 have been made by Teresa Quintel, “Interoperability of EU Databases and Access to Personal Data by National Police Authorities under Article 20 of the Commission Proposals”, *European Data Protection Law Review*, No. 4, 2020, pp. 470-482. However, we will take the distance from some of the author’s statements.

comparisons, while in reality its usage may also ultimately support the verification of an identity if, following its consultation, the CIR reveals that the individual is who they claim to be. If by consulting Article 20 a person results in not being who they claim to be, then, a fraudster or a victim of fraud has been detected.

Whether using fingerprints or facial images, the CIR can be queried with biometrics ‘taken live’ during an identity check²⁷¹. Thus, long-distance biometric checks cannot be performed under Article 20, as the procedure must be ‘initiated’ – but not ‘exhausted’ – in the presence of the person²⁷². Provided that contactless identification systems encourage arbitrary surveillance²⁷³ and seriously threaten human rights and the rule of law principle, we believe that this safeguard is really positive. In addition, in cases where biometrics cannot be used – e.g., because of a disability – or if such a query fails, the CIR could be consulted using the identity data of the person in combination with travel document data, or with the sole identity data if the third country national does not have a travel document – e.g., asylum seekers fleeing persecution.

²⁷¹ Article 20(2) of the IO Regulations.

²⁷² The use of ‘remote biometric identification’ arises serious concerns in the Joint Opinion of EDPB-EDPS No. 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (*Artificial Intelligence Act*), Brussels, 18.06.2021, p. 2 ff., commenting the European Commission Proposal on AI. In their words: ‘Remote biometric identification of individuals in publicly accessible spaces poses a high-risk of intrusion into individuals’ private lives, with severe effects on the populations’ expectation of being anonymous in public spaces’. Thus, a general ban on AI applicable to automated recognition of human features in publicly accessible spaces, as well as on the use of AI to categorise individuals from biometrics into clusters according to ethnicity, gender, political or sexual orientation, and other grounds for discrimination. Also, the EDPB and the EDPS condemned the use of AI to infer emotions from a natural person.

²⁷³ See “Le groupe Verts/ALE au PE appelle à la prudence concernant la surveillance biométrique et comportementale au sein des États membres”, *Bulletin Quotidien Europe*, No. 12819, 26.10.2021, denouncing that mass surveillance systems based on the use of biometric technologies are not proven to be efficient to fight crime and, consequently, calling on a moratorium to further discuss its usage.

Lea Tolstoy
F
08/10/1952
RUS 76543210

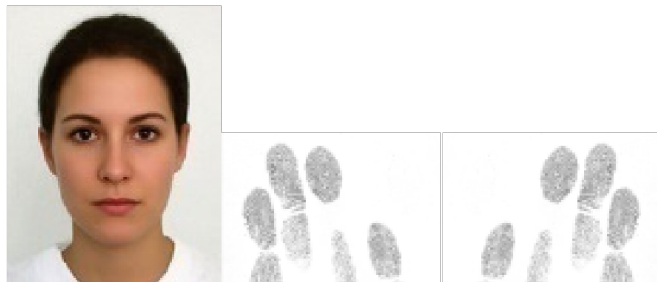


Figure 8 Identification according to Article 20 – Source: Own elaboration from the author's time working at the European Commission.

The authorities allowed to use the CIR by virtue of Article 20 are those falling within the meaning of Article 3(7) LED²⁷⁴ that – we recall²⁷⁵ – includes:

‘(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security’²⁷⁶.

Article 3(7) LED adopts a very broad definition, intentionally chosen by the co-legislators to model Article 20 regarding the Member States’ needs so that the latter must choose the authorities making use of the system along the lines of the ‘authority-user’²⁷⁷ principle. Despite this, while Article 3(7) LED is circumscribed to national authorities competent in the field of public security, as well as bodies and entities entrusted with public functions, Article 20 of the IO Regulations seems to have a wider scope as far as police authorities are empowered to:

- contribute to the prevention and the combating of illegal immigration, and

²⁷⁴ Article 4(19) of the IO Regulations.

²⁷⁵ See Chapter I.

²⁷⁶ Note that the Proposal for a Council Recommendation on operational police cooperation, COM(2021) 780 final, Brussels, 8.12.2021, p. 14, wants to grant law enforcement the access to national, EU, and international databases during cross-borders operations by, among others, carrying out identity checks.

²⁷⁷ According to Article 71(1) of Regulation (EU) 2019/817 and 67(1) of Regulation (EU) 2019/818, national authorities using or accessing the CIR are to be notified to eu-LISA that must publish – and update – the correspondent list on the *OJ* three months from the date on which each Interoperability component commences its operations. The European Commission, for its part, is in charge of notifying Member States and persons through its website.

- contribute to a high level of security within the AFSJ of the Union, including the maintenance of public security and public policy and safeguarding security in the territories of the Member States.

Therefore, Article 20 can be used not only for reasons of public security, but also for illegal immigration purposes, provided that the national ‘police authority’ is in charge of its management. The combination of migration and security goals under the interoperability roof confirms the co-legislators’ tendency to blur the lines between freedom, security and justice policies in the operational layer to finally criminalise the migration phenomenon. According to Quintel:

‘The Interoperability Regulations could be seen as final step in a sequence of measures that suggest relying on information stored in large-scale IT-systems to mitigate security concerns associated with migration’²⁷⁸.

Notably, Article 20 highlights that its usage must occur in full respect of the principle of non-discrimination. Consequently, individuals who cannot have their biometrics read cannot be treated differently do those who can, and any identity check on a third country national should be performed under the same conditions for which national databases are consulted to identify EU citizens or residents: ‘Otherwise, the Proposals would clearly seem to establish a presumption that third country nationals constitute by definition a security threat’²⁷⁹.

In addition, the co-legislators introduced an important safeguard for children by which the CIR cannot be consulted according to Article 20 in cases of children below the age of twelve. The IO Regulations do not explain how a search in the CIR according to Article 20(1) will “filter” the identity files stored therein so as not to provide information on children under twelve, yet this “filter” is surely feasible from a technical perspective. Conversely, it is not clear if this threshold should be respected by the ESP itself while querying and retrieving the information. In addition, the existence of this threshold reduces the contribution Article 20 could have brought to tracking missing and abducted children. According to the FRA, if Article 20 is to bring any added value to the detection of vulnerable children it will require enhanced cooperation between police and child protection authorities so that Article 20 ‘[...] should be complemented by tailored training for practitioners who may encounter children at risk’²⁸⁰.

²⁷⁸ Teresa Quintel, 2020, *op. cit.*, p. 206.

²⁷⁹ Opinion of the EDPS No. 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, Brussels, 18.04.2018, p. 14.

²⁸⁰ FRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Vienna, 2018, p. 12.

The CIR responds to Article 20's queries through the retrieval of alphanumeric, travel documents, and biometric data – i.e., with a 'picture' of the person. Specifically, if the consultation with the CIR is fruitful, the police authority is authorised to consult the data listed under Article 18(1) of the IO Regulations, that is the 'identity triangle', which consists of:

- identity data (name, surname, gender, date of birth);
- travel document data (number, issuing country, date of expiry), and
- biometric data (facial images, fingerprints).

In practice, the authority will receive the information without knowing its origin, which leads to a new *sui generis* form of 'access right' granting police authorities access to personal data that is stored in systems they may not usually have access to.

In general terms, identification *tout court* is neither a competence, nor an objective conferred on the EU by its Member States within the AFSJ, which raises doubts regarding the lawfulness of Article 20 *vis-à-vis* the founding Treaties. The execution of identity checks has been evaluated by the CJEU *vis-à-vis* the Schengen Borders Code, whose Article 23(a) makes it clear that the establishment of an area of free movement without controls at the internal borders must not affect 'the exercise of police powers by competent authorities of the Member States under national law'²⁸¹. As the CJEU sentenced:

'Article 21(a) of [the previous Schengen Borders Code] provides that the abolition of border control at internal borders is not to affect the exercise of police powers by the competent authorities of the Member States under national law, in so far as the exercise of those powers does not have an effect equivalent to border checks; that is also to apply in border areas'²⁸².

In these terms, identity checks executed within the Member States' territories and, consequently, at their internal borders as well, should be differentiated from those executed at

²⁸¹ Article 23(a) of the Schengen Borders Code. Previously, in C-378/97, *Florus Ariël Wijsenbeek*, 21 September 1999, EU:C:1999:439, the CJEU sentenced that 'as Community law stood at the time of the events in question' (para. 45) a Member State could require a person – whether a citizen or a third country national – to establish his nationality upon his/her entry from another Member State's territory. Also, it legitimated the imposition of penalty – comparable to those used at the national level and, in any case, proportionated – in case the person at issue refused to show an identity document. However, this judgment has become obsolete before the development of the EU legislation in the AFSJ as the CJEU ruled in C-368/20 and C-369/20, *NW v Landespolizeidirektion Steiermark (C-368/20), Bezirkshauptmannschaft Leibnitz (C-369/20)*, 26 April 2022, EU:C:2022:298, paras. 96-98, prohibiting the Member State to oblige a person, on pain of a penalty, to present a passport or identity card on entering its territory via an internal border. However, the CJEU limited such a prohibition to those cases 'when the reintroduction of the internal border control in relation to which that obligation is imposed is contrary to that provision' (para. 98).

²⁸² See C-278/12 PPU, *Atiqullah Adil v Minister voor Immigratie, Integratie en Asiel*, 19 July 2012, EU:C:2012:508, para. 53, on measures equivalent to border checks at 20 kilometres from the common border implemented by The Netherlands with the state party to the Convention implementing the Schengen Agreement establish the identity, nationality and/or residence status of the person stopped.

the external ones²⁸³. In *Atiqullah Adil v Minister voor Immigratie, Integratie en Asiel*, the CJEU ruled that the Schengen Borders Code did not affect national provisions empowering police authorities to check whether the obligations laid down by law to hold, carry, and produce papers and documents were fulfilled²⁸⁴. Nevertheless, any national legislation granting police authorities the power to check documentation ‘solely within an area of 20 kilometres from the land border of that State with States party to the Convention implementing the Schengen Agreement, the identity of any person, irrespective of his behaviour and of specific circumstances giving rise to a risk of breach of public order, in order to ascertain whether the obligations laid down by law to hold, carry and produce papers and documents are fulfilled’ is incompatible with the Schengen Borders Code, as it does not provide the guarantee that checks are not in effect the same as those undertaken at the external borders²⁸⁵.

Notably, in *Atiqullah Adil v Minister voor Immigratie, Integratie en Asiel*, the CJEU clarified that the nature of the checks conducted within the territories of the Member States *vis-à-vis* the checks performed at the borders should be assessed depending on: first, the frequency and selectivity of the checks made on the basis of general information and, second, the experience of persons illegally staying in the Member States’ territories. The CJEU maintained that the suppression of checks at the internal borders should not affect the Member States’ coercive power, and that checks at the internal borders must be distinct from those at the EU external borders so as to not hamper the establishment of a free movement area. Thus, the current Article 23(a) of the Schengen Borders Code sets forth that internal checks must not have an effect equivalent to border checks when:

- they do not have border controls as an objective;
- they are based on general police information and experience regarding possible threats to public security and aim, in particular, to combat cross-border crime;
- they are devised and executed in a manner clearly distinct from systematic checks on persons at the external borders, and

²⁸³ José Alejandro del Valle Gálvez, “Las fronteras de la Unión – El *modelo europeo* de fronteras”, *Revista de Derecho Comunitario Europeo*, Vol. 6, No. 12, 2002, pp. 299-341, p. 326 ff., points out that the EU borders model includes both internal and external ones: ‘[...] internal and external borders, which are mentioned in the Treaties and in secondary law, always in the plural, are borders that already exist (certain land borders of the States) or that are artificially legally constructed by the EU (certain ports and airports). This implies that internal and external borders do not have conceptual autonomy as a legal category outside of Union Law, since they need state and EU construction for their definition, and are not operative for other national or international legal purposes, since they have been listed, assigned and functionally created to meet a specific objective, common to the States, the EC and the EU: the Area of Freedom, Security and Justice’ (our own translation). The author stresses that in the EU internal borders are prodromic to the establishment of an internal market, while the external ones are ‘accompanying measures’ to the former.

²⁸⁴ C-278/12 PPU, *Atiqullah Adil v Minister voor Immigratie, Integratie en Asiel*, para. 71.

²⁸⁵ *Ibid.*, para. 75.

- they are carried out as spot-checks²⁸⁶.

The latest Proposal advanced by the European Commission to amend the Schengen Borders Code²⁸⁷ would expressly refer, as far as the general police information and experience requisite is concerned, to the possibility of using ‘monitoring and surveillance technologies’ within the territory, not only for ‘public security’ reasons but also for ‘public policy’ objectives²⁸⁸ so as to include:

- the combat of cross-border crime;
- the combat of illegal stays linked to illegal immigration, or
- efforts made to contain the spread of an infectious disease with epidemic potential as detected by the European Centre for Disease Control in cooperation with national authorities.

For this purpose, the new Schengen Borders Code is expected to set up joint police patrols competent to execute check on irregular migrants, among others. In parallel, Article 23 should also exclude from the list of checks that have no equivalent effect to those performed at the borders:

- those conducted in a non-systematic manner at transport hubs, or directly on board of passenger services and when they are based on risk analysis, and
- those realised on the basis of ‘monitoring and surveillance technologies generally used in the territory, for the purposes of addressing threats to public security or public policy’²⁸⁹.

In these terms, the new Schengen Borders Code would widen its scope so as to include identity checks for migration and public health purposes: the former, is expected to contribute to reduction of unauthorised secondary movements; the latter, seeks to contain the spread of highly contagious diseases such as COVID-19²⁹⁰.

Other checks covered by Article 23(b), (c), and (d) of the Schengen Borders Code are:

²⁸⁶ Article 23(a) of the Schengen Borders Code. These conditions were proposed by the European Parliament following the CJEU’s judgments C-188/10 and C-189/10, *Aziz Melki and Sélim Abdeli*, para. 70.

²⁸⁷ See the Council of the EU, 7751/19, Brussels, 25 April 2019, pp. 82-83. Another proposal was presented by the European Commission in 2017, but no agreement could be reached within the Council of the EU – see the “Sylvie Guillaume désignée rapporteur sur la réforme du Code frontières Schengen”, *Bulletin Quotidien Europe*, No. 12912, 17.3.2022.

²⁸⁸ Council of the EU, *Proposition de règlement du Parlement européen et du Conseil amendant le règlement (UE) 2016/399 concernant un code de l’Union relatif au régime de franchissement des frontières par les personnes - Compromis partiel de la présidence*, Brussels, 6366/22, 18 February 2022, p. 6.

²⁸⁹ Article 23(a)(iii)(iv) of the proposed amendment to the Schengen Borders Code.

²⁹⁰ Note that Article 4(2)(k) TFEU confers the EU competence ‘on common safety concerns in public health matters, for the aspects defined in this Treaty’.

- security checks carried out on persons at ports and airports by the competent authorities under the law of each Member State, by port or airport officials or carriers, provided that these checks are also carried out on persons travelling within a Member State²⁹¹;
- individual checks stemming from an obligation to hold or carry papers and documents set forth by national law, and
- the possibility for a Member State to legally provide for an obligation to report the presence of third-country nationals within its territory pursuant to the provisions of Article 22 of the Convention implementing the Schengen Agreement²⁹².

Should the new Schengen Borders Code Proposal be adopted²⁹³, Article 23 will also enable ‘checks for security purposes of passenger data against relevant databases on persons traveling in the area without controls at internal borders which can be carried out by the competent authorities under the applicable law’, while the security checks mentioned in Article 23(b) will be reformulated in a broader manner so as to cover not only ports and airports, but any transport hub provided that the competent authorities or carriers also deploy the same checks on persons travelling within the Member State.

The rationale underpinning Article 23 of the Schengen Borders Code is found in the Member States’ willingness to circumscribe the EU operational competence on borders and to keep their sovereign prerogative on the execution of checks on immigrants²⁹⁴. We should recall, as Prof. García Andrade does, that²⁹⁵ ‘[...] the interest of the EU and its Member States on borders should not be found in the normative cooperation but in a technical and operational one’²⁹⁶. Despite the provisions of Protocol No 23 on the Member States’ external relations with regard

²⁹¹ Article 23(b) of the Schengen Borders Code.

²⁹² Article 23(d) of the IO Regulations.

²⁹³ Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 on a Union Code on the rules governing the movement of persons across borders, COM(2021) 891 final, Strasbourg, 14.12.2021.

²⁹⁴ Notably, Article 45(1) of CFREU guarantees the right to move and reside freely within the territory of the Member States to Union citizens. Its second paragraph, instead, sets forth that third-country nationals who reside legally in the EU may be granted those rights in accordance with the founding Treaties. Therefore, Member States have been adopting domestic legislations providing for the implementation of identity checks to verify the legality of third country nationals’ presence within the Schengen area. In this sense, the forthcoming Schengen Borders Code is expected to regulate ‘the possibility for a Member State to provide by law for an obligation for third-country nationals to report their presence on its territory and an obligation for managers of accommodation establishments to ensure that third-country nationals complete and sign registration forms’ according to “Les ministres de l’Intérieur de l’UE auront un premier débat d’orientation le 3 mars sur la réforme du Code frontières Schengen”, *Bulletin Quotidien Europe*, No. 12897, 24.2.2022, (our own translation). However, the gordian knot to untie is how to comply with the Schengen Border Code dispositions and, above all, how to exercise this power without affecting the freedom of movement and residence fully enjoyed by EU citizens.

²⁹⁵ Paula García Andrade, 2015, *op. cit.*, pp. 228-236, and pp. 360-387.

²⁹⁶ *Ibid.*, p. 364 (our own translation).

to the crossing of external borders²⁹⁷, the EU competence on border checks and on their integrated management is of shared nature. Therefore, the principle of pre-emption regulates the exercise of such a competence between the EU and its Member States. Yet, unlike Prof. García Andrade²⁹⁸, we believe that shared competences can also have a place in the operational layer²⁹⁹. In fact, the use of coercive powers by the EBCG Agency, in foreign lands, has now become tangible thanks to the possibility for the EU to conclude the so-called status agreements³⁰⁰. The expanding power of the EBCG Agency is putting into question the Member States' monopoly in the operational layer, so that a sort of 'mixed' execution made of Member States' authorities and Union agency staff is now possible. However, we should highlight that by 'making safe' certain types of identity checks, Article 23 of the Schengen Borders Code is legislating on the matter and, consequently, is enabling the EU to creep into the 'Member States' territories' should the CJEU support this position³⁰¹.

These beliefs help us to understand the European Commission's statement on Article 20 for which:

'The identification of undocumented or insufficiently documented persons by a police officer does not necessarily have to be an act of migration management or law enforcement in the strict definition of the VIS, Eurodac, EES and proposed ETIAS legal instruments (the two cases provided for in the existing legal bases of these systems). It should also be possible to undertake them within the scope of the police competences determined by national law. For this identification, the person is physically present and is presumed innocent. The aim is simply for the competent authorities to be able to address the person by their name'³⁰².

The identification of undocumented, or insufficiently documented, persons by a police officer for migration management or for law enforcement purposes within the Member States'

²⁹⁷ According to it: 'The provisions on the measures on the crossing of external borders included in Article 77(2)(b) of the Treaty on the Functioning of the European Union shall be without prejudice to the competence of Member States to negotiate or conclude agreements with third countries as long as they respect Union law and other relevant international agreements'.

²⁹⁸ Paula García Andrade, 2018, *op. cit.*, p. 168:

'Member States still retain the power to implement or execute border controls. Although conventional powers usually present prescriptive character, this execution power on borders constitutes, in my view, the relevant function involved in the arrangements agreed with third countries regarding the deployment of joint border patrols, a task which is still in the hands of Member States in spite of the recent reform of the Frontex Agency'.

²⁹⁹ See Chapter VI.

³⁰⁰ *Ibidem*.

³⁰¹ See, *mutatis mutandi*, C-368/20 and C-369/20, *NW v Landespolizeidirektion Steiermark (C-368/20), Bezirkshauptmannschaft Leibnitz (C-369/20)*, para. 86: 'However, as the Court has held, the only articles in which the FEU Treaty expressly provides for derogations applicable in situations which may affect law and order or public security are Articles 36, 45, 52, 65, 72, 346 and 347, which deal with exceptional and clearly defined cases. The derogation provided for in Article 72 TFEU must, as is stated in settled case-law, be interpreted strictly. It follows that Article 72 TFEU cannot be read in such a way as to confer on Member States the power to depart from the provisions of EU law on the basis of no more than reliance on the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security [...]'.
³⁰² Commission Staff Working Document Impact Assessment, SWD(2017) 0473 final, Strasbourg, 12.12.2017.

territories is a field of competence “operationally” retained by the Member States and, as such, it is regulated by domestic law. The lack of operational competence in this regard would justify, in our eyes, the fact that Member States may express their willingness to opt-in to such a measure or not³⁰³. If Member States decide to incorporate Article 20, then the co-legislators require them to:

- designate the competent police authorities that will access the CIR for the purpose of Article 20;
- lay down the procedures, conditions, and criteria of the checks performed under Article 20, and
- specify the purposes for which the CIR can be consulted according to Article 2(1)(b) and (c) of the IO Regulations.

The integration of Article 20 in the Member States’ domestic orders can be fulfilled by adopting a new legal text if required; in any case, national laws must clearly indicate that they cover the scope of Article 20. As Prof. Vavoula notes, the non-binding character of Article 20 risks leading to a fragmented implementation of the IO Regulations that ‘may be prone to abuses, misunderstandings and arbitrary or unclear designations’³⁰⁴. Given this assumption, we would add that while opting for a “soft solution”, the co-legislators have circumvented the limits foreseen by the founding Treaties – first of all, Article 72 TFEU – as the EU has not been recognised as having competences for support, coordination, and supplement as far as police checks within the Member States’ territories are concerned. Although the ability to insert soft provisions in an instrument that is directly applicable within the Member States’ domestic orders is not a new legislative practice, Article 20 contradicts the binding effect of the legislative texts chosen by the co-legislators – i.e., a regulation instead of a directive – as its IO Regulations set forth that: ‘This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties’³⁰⁵. It must be recalled that, according to the CJEU’s settled case-law:

‘[...] pursuant to Article 288 TFEU and by virtue of the very nature of regulations and of their function in the system of sources of EU law, the provisions of those regulations generally have immediate effect in the national legal systems without its being necessary for the national authorities to adopt measures of application. Nonetheless, some of those

³⁰³ Article 20(2), (5), and (6) of the IO Regulation. Some Member States, like Croatia, adopted a new legislation. Others, like France, amended its domestic law. Only Denmark, as far as we know, did not opt-in into this measure which shows off the willingness of the delegations to support this norm.

³⁰⁴ Niovi Vavoula, 2020, *op. cit.*, p. 148.

³⁰⁵ Article 79 of Regulation (EU) 2019/817 and Article 75 of Regulation (EU) 2019/818, *in fine*, in both cases.

provisions may necessitate, for their implementation, the adoption of measures of application by the Member States³⁰⁶.

Yet, in practice, this is not really the case: Article 20 does not leave the Member States any margin of manoeuvre regarding the means of its implementation, but leaves them free to adopt, or not, such a measure while providing the tools for its put into motion.

The competence gap stemming from Article 20 has not been sufficiently highlighted so far, maybe because it has been supported by the Member States themselves and because of the European Commission's efforts to realise police checks³⁰⁷. It could be alleged that, in reality, Article 20 of the IO Regulations is underpinned by the EU competence on the establishment of an area without any control on persons crossing internal borders, whatever their nationality – see Article 77(2)(e) TFEU – or on the EU competence to combat illegal migration³⁰⁸ – which would find its foundation in Article 79(2)(c) TFEU. However, police authorities will know whether a migrant is illegally staying within the territory of a Member State or not by accessing the underlying IT systems – i.e., the EES – if, and only if, they are allowed to access them. Consequently, this interpretation would fall short *vis-à-vis* the “policy-neutral” application of Article 20 that has the identification of individuals, notwithstanding their criminal or illegal activity, as its main objective. Besides, from a competential perspective, there cannot be any ‘neutral legislation’: any EU regulation must be underpinned by a legal basis foreseen by the founding Treaties conferring on the EU the power to act in a specific domain. Referencing the functionalist theory is not sufficient to justify the adoption of an act pursuing a concrete goal unless the co-legislators apply the non-provision clause³⁰⁹. Whatever legal basis is chosen, Article 72 TFEU will always present a crucial limitation to Article 20 as it preserves the Member States’ responsibility to maintain law and order and to safeguard internal security³¹⁰.

From the analysis made above, the EU intervention in the performance of individual checks within the Member States’ territories does not seem to be underpinned by any legal basis regarding the AFSJ unless the reach of the EU competence on borders – i.e., Article 77(2)(b) and (d) TFEU – is so stretched to overlap with the scope of EU migration and security policies. Yet, in no way does the current Schengen Borders Code require the ‘identification’ of the

³⁰⁶ See the judgment of C-528/15, *Al Chodor*, 15 March 2017, EU:C:2017:213, para. 27 and the case-law quoted therein.

³⁰⁷ Commission Recommendation of 12.5.2017 on proportionate police checks and police cooperation in the Schengen area, C(2017) 3349 final, Brussels, 12.5.2017.

³⁰⁸ See C-278/12 PPU, *Atiqullah Adil v Minister voor Immigratie, Integratie en Asiel*, para. 55.

³⁰⁹ Article 352 TFEU.

³¹⁰ See C-278/12 PPU, *Atiqullah Adil v Minister voor Immigratie, Integratie en Asiel*, para. 52. This is driving the EU legislation at the limits of paradox. Looking at the screening Regulation, for instance, where the EU legislator is extending the concept of border checks so as to justify identity controls within the Member States.

individual in the terms of Article 20, which depict identification as more than a tool for pursuing freedom, security and justice objectives³¹¹. Article 20 does not circumscribe its scope of application as it does while designating, for example, the authorities eventually authorised to use it. As a general rule, police authorities³¹² will be able to identify undocumented migrants or verify an identity claim by accessing the CIR³¹³ in one of the following circumstances:

- where a police authority is unable to identify a person due to the lack of a travel document or another credible document proving that person's identity;
- where there are doubts:
 - about the identity data provided by a person;
 - as to the authenticity of the travel document or another credible document provided by a person – in cases where documents may have been forged³¹⁴;
 - as to the identity of the holder of a travel document or of another credible document³¹⁵, or
- where a person is unable (e.g. they are unconscious), or refuses, to cooperate³¹⁶.

The cases above respond to the practical needs or, in the CJEU's words, follow the 'general information and experience' of national authorities³¹⁷ in the performance of identity checks within the territories of the Member States. Prof. Vavoula highlights how these clauses do not eliminate the fact that the objectives pursued by Article 20 are still too broadly formulated³¹⁸. However, we cannot discount them as they limit the scope of application of Article 20 and prevent its routine use. In the European Commission's eyes:

‘While this requires establishing end-user access-rights, these data will normally be found in a passport and no other data (i.e. the additional information) will be provided; police authorities will not know if this identity data came from VIS, Eurodac, EES, ETIAS or the ECRIS-TCN system’³¹⁹.

Article 20 infers that the consultation of the CIR for identification purposes should be used as a sort of *ultima ratio* in case the police do not know if the individual has a file open in the VIS or the ETIAS, for example. From our perspective, the co-legislators should better specify

³¹¹ Opinion of the EDPS No. 4/2018 on *the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, Brussels, 18.04.2018, p. 13.

³¹² Article 4(19) of the IO Regulations and our comments *supra*.

³¹³ See the analysis of Teresa Quintel, 2020, *loc. cit.*

³¹⁴ It may happen that a person shows a forged travel document or a document that does not correspond to the person in front of the authority.

³¹⁵ Whenever a person shows a document, and the police has doubts upon his/her identity because it does not correspond to the person in front of the authority.

³¹⁶ See Article 20(1).

³¹⁷ See C-278/12 PPU, *Atiqullah Adil v Minister voor Immigratie, Integratie en Asiel*, para. 89.

³¹⁸ Niovi Vavoula, 2020, *op. cit.*, p. 144 ff.

³¹⁹ Commission Staff Working Document Impact Assessment, SWD(2017) 0473 final, Strasbourg, 12.12.2017.

the subsidiarity character of Article 20 *vis-à-vis* the underlying IT systems in order to emphasise the prohibition from using it in a systematic manner, which would be in opposition to the limits established under Article 23 Schengen Borders Code.

Another point of discussion should be raised on Article 20(4) of the IO Regulations, according to which:

‘Where a police authority has been so empowered by national legislative measures as referred to in paragraph 6, it may, in the event of a natural disaster, an accident or a terrorist attack and solely for the purpose of identifying unknown persons who are unable to identify themselves or unidentified human remains, query the CIR with the biometric data of those persons’.

When presenting the interoperability objectives, we highlighted that the IO Regulations ‘almost’ undertake the (multi-)purposes pursued by large-scale IT systems. Our concerns are directed at Article 2(1)(g) of the IO Regulations, that aims at facilitating ‘[...] the identification of unknown persons who are unable to identify themselves or unidentified human remains in case of a natural disaster, accident or terrorist attack’³²⁰. This is the sole purpose that cannot be attributed to any underlying large-scale IT system. The lawfulness of such a data processing activity can be justified in the light of Article 6(1)(d) GDPR, that does not require the consent of the data subject when the processing of personal data goes to the vital interest of the data subject or of another natural person³²¹, that is, in cases where the ‘processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters’³²². However, this further data processing activity should have been flagged by the co-legislators if it adds a new purpose to those already pursued by the underlying IT systems and its compatibility should have been assessed in full respect of the principle of purpose limitation³²³. Moreover, its insertion is hardly justifiable in light of the EU competence’s catalogue regulated under the AFSJ and, lastly, this puts into question its validity within the interoperability objectives.

On closer inspection, the identification of disaster victims and unidentified bodies is not a new goal pursued by the EU: in lack of comprehensive databases on EU citizens, in 2005 the European Commission proposed to establish a European register for travel documents and ID

³²⁰ This objective was added during the negotiation – see the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 - Examination of the Presidency revised text*, 7651/18, Brussels, 13 April 2018, pp. 3 and 18.

³²¹ Article 6(1)(d) GDPR.

³²² See recital (46) GDPR.

³²³ See Chapter I.

cards, and a European Criminal Automated Fingerprints Identification System (EU-AFIS)³²⁴. It must be presumed that the ‘provisions concerning passports, identity cards, residence permits or any other such document’ can be adopted by the EU to ensure the absence of any control on persons crossing internal borders³²⁵, whatever their nationality, which considerably limits the EU’s empowerment to legislate in this field. Besides, Article 77(3) TFEU requires a special legislative procedure and the unanimity of the Council, which might discourage the submission of a proposal by the European Commission based upon the Article. If so, issues of the horizontal allocation of competences arise, as the purpose pursued by Article 2(1)(g) of the IO Regulations should be found, in our view, in Article 196 TFEU. According to this norm:

‘1. The Union shall encourage cooperation between Member States in order to improve the effectiveness of systems for preventing and protecting against natural or man-made disasters.

Union action shall aim to:

(a) support and complement Member States’ action at national, regional and local level in risk prevention, in preparing their civil-protection personnel and in responding to natural or man-made disasters within the Union;

(b) promote swift, effective operational cooperation within the Union between national civil-protection services;

(c) promote consistency in international civil-protection work.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure shall establish the measures necessary to help achieve the objectives referred to in paragraph 1, excluding any harmonisation of the laws and regulations of the Member States’.

Civil protection is an EU competence intentionally placed outside the AFSJ as Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism confirms by expressly excluding the health, as well as the home affairs and justice fields from its range of application³²⁶. The pursuit of an objective different from that of the legal bases used follows the trend undertaken by the EU, for example, in the development and security fields³²⁷, with consequent breaches of the subdivision of competences set forth in EU primary law. According to the CJEU, the necessity and opportunity to insert Article 196 TFEU should be based on objective factors amenable to judicial review. If the *PCA Philippines* case is taken as a valid precedent, Article 196 TFEU could be considered as an

³²⁴ Peter Hobbing, *An analysis of the commission communication (COM (2005) 597 final of 24.11.2005) on improved effectiveness, enhanced interoperability and synergies among European databases in the area of justice and home affairs*, IP/C/LIBE/FWC/2005-08, Brussels, 14.02.06, p. 11.

³²⁵ Article 77(3) TFEU.

³²⁶ Article 1(6) of Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism Text with EEA relevance, *OJ L* 347, 20.12.2013, pp. 924-947.

³²⁷ Paula García Andrade, 2018, *op. cit.*, p. 178.

objective that is distinct from the other EU policies pursued by the IO Regulations for being ‘[...] neither secondary nor indirect in relation to the latter objectives’³²⁸. In this case, the CJEU referred to extensive ‘obligations’ in order to assess whether readmission, transport, and environment constituted separated objectives pursued by the EU *vis-à-vis* that of development cooperation which underpinned the Framework Agreement on Partnership and Cooperation with the Republic of the Philippines. In these terms, we might appreciate that Article 196 TFEU does not integrate the wide legal framework supporting the IO Regulations. However, Prof. García Andrade criticised the Court’s position by affirming that:

‘If readmission obligations are substantially specific in relation to development cooperation, those clear obligations should have been based, according to the principle of conferral, on the Treaty provision on readmission; the way those obligations are further implemented constitutes a different issue to be solved through the appropriate execution measures’³²⁹.

Therefore, if Article 20(4) of the IO Regulations is found to be ‘substantially specific’ *vis-à-vis* freedom, security and justice policies, then, Article 196 TFEU should integrate the IO Regulations’ legal frameworks. In case its provision as a ‘correct legal basis’ cannot be supported, we should anyway question the lawfulness of Article 20(4) TFEU provided that, in the civil protection field the EU has only a supportive competence that excludes any kind of harmonisation³³⁰. Thus, further concerns arise because of the procedural incompatibility of Article 196 TFEU with the other legal bases underpinning the IO Regulations³³¹.

The fact that the scope of application of the IO Regulations breaches Article 196 TFEU is somewhat lessened by the fact that Member States may decide whether to avail themselves of such a provision or not. It seems to us that the lack of sufficient empowerment has been “overcome” by the co-legislators through the ‘soft norm’ expedient. Adherence to Article 20(4) requires a specific action on the Member States’ behalf in order to enable their national authorities to make use of it. Provided that the adherence is made in a ‘separate’ form with respect to the whole of Article 20, the norm is relegated to, if not on a secondary, at least a separate layer with regard to the other paragraphs of Article 20. Such a configuration (intentionally?) strengthens the challenge found in the fourth paragraph, though this should not be excluded *tout court* if it is considered that Article 2(1) of the IO Regulations does not establish any hierarchy among the objectives pursued by the Regulations and, conversely, it

³²⁸ C-377/12, *European Commission v Council of the European Union*, 11 June 2014, EU:C:2014:1903, para. 59.

³²⁹ Paula García Andrade, 2018, *op. cit.*, p. 180.

³³⁰ Article 6(f) TFEU. As we analysed in Chapter II, this implies that the EU (implied) external action turns out to be exercised in parallel with the Member States ones.

³³¹ C-130/10, *European Parliament v Council of the European Union*, paras. 42 to 45.

places them on an equal footing. What may actually constitute an obstacle is the fact that the rationale used for hard law by the CJEU in *PCA Philippines* cannot be transposed to the soft norms and specifically to Article 20(6) of the IO Regulations. According to the latter:

‘Member States wishing to avail themselves of the possibility provided for in paragraph 4 shall adopt national legislative measures laying down the procedures, conditions and criteria’.

2.3.2. The access to the CIR for the detection of multiple identities: The purpose of Article 21

According to the Staff Working Document Impact Assessment conducted by the European Commission that accompanied the interoperability Proposals in 2017, the detection of multiple identities and the fight against identity fraud were among the main reasons behind the push to abandon the silo approach promoted by the fragmented development of large-scale IT systems³³². Article 21 leads the procedure for the detection of multiple identities and, in a nutshell, enables the finding of discrepancies between the declared identities in different systems, increasing the ability to identify identity fraudsters³³³. According to Article 21:

‘1. Where a query of the CIR results in a yellow link in accordance with Article 28(4), the authority responsible for the manual verification of different identities in accordance with Article 29 shall have access, solely for the purpose of that verification, to the data referred to in Article 18(1) and (2) stored in the CIR connected by a yellow link.

2. Where a query of the CIR results in a red link in accordance with Article 32, the authorities referred to in Article 26(2) shall have access, solely for the purposes of combating identity fraud, to the data referred to in Article 18(1) and (2) stored in the CIR connected by a red link’.

As the European Commission highlighted in the Staff Working Document Impact Assessment above mentioned, Article 21 adds a data processing activity that involves the personal data stored in the CIR and the SIS and the correspondent templates held in the sBMS. Thus, Article 21 focuses on yellow and red links as they provide for new access rights to the data stored in the CIR and the underlying IT systems according to the multiple-identity detection process. The multiple-identity detection process is extensive and must be interpreted in the light of Articles 25-36 of the IO Regulations³³⁴.

³³² Commission Staff Working Document Impact Assessment, SWD(2017) 0473 final, Strasbourg, 12.12.2017:

‘Repeated and separate storing of personal information in separate and unconnected systems makes it possible that people are recorded under different identities, without this being detected. Ultimately, as it has been reported, one person may end up having different identities recorded in SIS, Eurodac and VIS, while national authorities are unable to distinguish the cases where the difference points to identity fraud or to a regular situation (e.g. change of name, multiple nationalities etc.)’.

³³³ Note that large-scale IT systems already contemplate some internal forms to manage third country nationals’ identities: the Eurodac has links; the VIS has dossier reference numbers; the EES has traveler files, and the ETIAS has ‘linked applications’ with the exception of identical travel documents – see Chapter III.

³³⁴ Article 25 explains what is the MID, its purpose and composition. Article 26 explains who (which authorities) have access to the MID and its links. Article 27 sets forth the multiple-identity detection procedure as a three-

The multiple-identity detection procedure – or linked detection process, according to the Feasibility Study on a Common Identity Repository (CIR)³³⁵ – is triggered:

- as soon as a large-scale IT system is added to the interoperability architecture, and
- each time an identity file is created or updated in one of the underlying IT systems, including the Eurodac as soon as the European Commission's amended Proposal is adopted³³⁶.

The former situation is expected to occur as soon as the existing or future large-scale IT systems migrate into the interoperability infrastructure. The latter situation, instead, responds to situations occurring as soon as the interoperability components enter into operation³³⁷. We will firstly address the latter case to allow for an understanding of the entire multiple-identity detection procedure. However, before we begin, we shall highlight that in both cases the multiple-identity detection procedure pursues two main objectives:

- firstly, it seeks to facilitate the controls over *bona fide* travellers, and
- secondly, it aims to detect identity fraud used to access the Schengen area.

Identity frauds consist of two phenomena: identity thefts and false identities³³⁸. The former consists of the unlawful stealing of someone's identity, this results in an individual becoming a victim of the crime; the latter, instead, consists of the use of a bogus identity that hides the individual's true identity and that might be harmful to the state³³⁹. Identity theft and false identities are used to define persons committing a '[...] deliberate act of (unlawfully or without permission) obtaining, appropriating, possessing or creating false identification (and thereby committing an unlawful act or with the intention to commit unlawful acts)'³⁴⁰. Historically,

layered process: a comparison of biometrics in parallel with a comparison of alphanumeric identity data, and with travel document data. Article 28 establishes the results of the multiple-identity detection process – i.e., no result or link (automatic white or yellow). Article 29 provides the authorities responsible for the manual verification of different identities in case of yellow links, as well as the data they have to access in order to verify that link. Article 34 defines the identity confirmation file as the virtual entity containing the links related to a given identity in various systems, the reference to those systems, the authority responsible for the manual verification of the linked identities and a single identification number.

³³⁵ European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 57.

³³⁶ Article 27(1) of the IO Regulations.

³³⁷ See above.

³³⁸ Note that the SIS stores 'aliases' and information on 'misused identity': 'alias' occurs when a person uses a false or assumed identity; 'misused identity', instead, happens where a person, subject to an alert in SIS, uses the identity of another real person, in particular when a document is used to the detriment of the real owner of that document.

³³⁹ See Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law, *OJL* 198, 28.7.2017, pp. 29-41, and, for example Chapter II on "De las falsedades documentales" of the Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, *Boletín Oficial del Estado* No. 281, 24.11.1995.

³⁴⁰ See Bald de Vries, Jet Tigchelaar, Tina van der Linden, and Ton Hol, *Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen*. *Disciplinegroep Rechtstheorie*, Departement Rechtsgeleerdheid, University of Utrecht, 2007. Thus, the concept of identity fraud for the purposes of the IO Regulations includes identity theft and false identity.

these crimes have been committed through the use of a false document³⁴¹ – pseudo documents, forged documents, and counterfeited documents – and have become a major concern in the digital environment³⁴² and, in order to combat this threat, Europol and the EBCG Agency have joined their efforts³⁴³. The latter’s goal is crucial to maintaining a high level of security within the Schengen area and, specifically, to the fight against organised crime, terrorism, migrant smuggling, and trafficking in human beings³⁴⁴. In these terms, the multiple identity detection procedure is of great importance to PJCCM. However, we should not forget that this procedure often involves third country nationals who are not associated with criminals and who also might be in need of protection³⁴⁵: identity fraudsters may be asylum seekers fleeing their countries of origin, or migrants trying to illegally access the Schengen area without pursuing any criminal activity³⁴⁶.

a) The Multiple-Identity Detection procedure

As the multiple-identity detection procedure is comprised of two phases, where the former is an automated procedure, and the latter consists of manual verification, we will divide our analysis into two parts to assess the legal concerns stemming from each step.

³⁴¹ The terrorist attacks perpetrated in the EU in the last twenty years have been committed by persons using fake identities – e.g., in the Nice attacks a terrorist was found to have used almost thirty different identities. Identity fraud includes cases in which a third country national uses an EU identity, but also cases where an EU citizen use a third country national’s identity to perpetrate crimes within the Schengen area. The latter scenario is even more worrisome since EU citizens data are mainly stored in national databases and there is no possibility to crossmatch Member States’ databases.

³⁴² Note that morphed images allow to merge two people’s face images in one single picture that can be inserted in genuine passports – see, for example, Robin S. S. Kramer, “Face morphing attacks: Investigating detection with humans and computers”, *Cognitive Research: Principles and Implications*, Vol. 28, No. 4, 2019, and Europol, *Facing Reality? Law enforcement and the challenge of deepfakes*, Luxembourg, 2022, p. 12 ff. The authentication mechanism compares the facial image taken alive with the morphed picture without detecting inconsistency so that a forged passport would be quoted as valid travel document. To minimise those risks, identity checks based on facial recognition should compare the biometric templates taken alive and stored in a database with an individual’s facial image lively taken. The digitalisation of photographs, instead, should be excluded since this may not be reliable for biometric recognition purposes so we appreciate the fact that the sBMS does not store any of them. Besides, facial images stored in the passport chip could potentially be extracted from the passport chip and compared with the enrolled picture in the light of the one-to-one comparison, yet this possibility has also been excluded too to minimise false positives rates.

³⁴³ See Chapter III.

³⁴⁴ European Migrant Smuggling Center, *4TH ANNUAL ACTIVITY REPORT – 2020*, The Hague, 2020, available at www.europol.europa.eu.

³⁴⁵ FRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Vienna, 2018.

³⁴⁶ FRA, *Fundamental rights and the interoperability of EU information systems: borders and security*, Vienna, 2017, p. 8.

i) The automated procedure: The generation of white and yellow links

The creation, or updating, of an individual file in one of the underlying IT systems launches an automatic order to the interoperability components that must compare the newly added data with: the biometric data stored in the sBMS and the identity and travel document data stored in the CIR and the SIS according to probabilistic matching – i.e., through a one-to-many comparison³⁴⁷. In cases of biometrics, the templates stored in the sBMS are compared, rather than the data, and all the results are reported to the CIR³⁴⁸. When searching identity or travel document data, the CIR and, through the ESP, the SIS compare the newly added data with the existing data stored therein³⁴⁹. If the file is created or updated in the SIS, this system uses the sBMS to compare the templates stored within it – including the SIS templates – and the ESP to compare the biographical data stored in the CIR³⁵⁰. Thus, the MID supports the CIR³⁵¹ in determining the type of links to be generated among the different systems' identity files and stores the links in the identity confirmation file for future use³⁵². IT analysis confirms that the comparison occurs within the same category of data (fingerprints against fingerprints; facial images against facial images; identity data against identity data³⁵³, and travel document data against travel document data)³⁵⁴. Identity data must always be present. The comparison occurs

³⁴⁷ European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 3: 'In probabilistic matching, several field values are compared between two records and each field is assigned a weight that indicates how closely the two field values match. The sum of the individual fields weights indicates the likelihood of a match between two records'. In these terms: 'The CIR would act as a client of the sBMS, and the links it would create and store would depend on the horizontal biometric matching (probabilistic match) delivered by the sBMS'.

³⁴⁸ Article 27(2) of the IO Regulations 'The shared BMS shall compare the biometric templates obtained from any new biometric data to the biometric templates already contained in the shared BMS in order to verify whether data belonging to the same person are already stored in the CIR or in Central SIS'. Also, when the CIR creates or updates a record in the sBMS, a biometric identification is performed on all available biometric templates in the sBMS. When the CIR record contains biometrics, it might create yellow links or automatic white in the MID.

³⁴⁹ The CIR will perform a biographic search within the CIR and request a search in SIS via the ESP. All results of this search should be evaluated and compared by the CIR. Possible yellow links or automatic white links will be created in the MID by the CIR.

³⁵⁰ In any case, it is the CIR that evaluates and compares the results stemming from the sBMS, the CIR, and the SIS. Indeed, to perform a multiple-identity detection against or from the SIS, the alert must be provided of both identity data and travel document data.

³⁵¹ It is the CIR that detects new identities and decides whether a white/yellow link should be created. The CIR itself instructs the MID of the links created in the identity confirmation file. However, the competent authority in charge of the manual verification procedure interacts with the MID to convert the yellow links.

³⁵² It also stores the reference to that authority in charge of the manual verification – i.e., the one that decide to turn a yellow link in a specific color – the date and hour he/she did it.

³⁵³ Thus: names will be compared with names (including surname and first name); date of birth will be compared with date of birth; gender will be compared with gender, nationality and place of birth will be compared with nationality and place of birth.

³⁵⁴ These are not the identity data contained in the document but the type, number, expiring date, issuing country of the travel documents. To match, the following values must be identical: type of document; three letter country code, and document-number. In the case of the SIS, only data on passports shall be used, but biographical data can be: confirmed identity, where the person's identity has been confirmed; not confirmed identity, where there is not

among data belonging to different systems and not within each system³⁵⁵ and must terminate before the new record – i.e., the data – is created or updated. Only one link can be established between two individual files, including when a person has more than one individual file stored within a single system³⁵⁶. What is expected from this comparison is the establishment of colour-coded links indicating whether the data matches with what is stored in the systems. If no match is found (\emptyset), the procedure must continue according to the instrument governing it. The creation of links, instead³⁵⁷, considers four different scenarios:

- first, multiple justified identities, or
- second, cases of unclear identities, which may flow into:
 - multiple unjustified identities;
 - different individuals with similar identities, or
 - multiple justified identities.

As a general rule, the former scenario results in the creation of a white link; cases of unclear identities, instead, give rise to a yellow link. The possibility to generate links and to assign different colours depends on the establishment of predetermined thresholds that define “matches”³⁵⁸ among identity data, travel document data, and biometric similarities³⁵⁹.

The compared data might be the same (=) or similar (\approx), this will result in a white link being generated in an automated manner³⁶⁰. If a 100% match is found between the data stored in two different EU information systems, then, the match is considered to be equal, and the automatically generated white link would point out that the data stored in the CIR or the SIS

sufficient proof of the person’s identity; alias for false or assumed identity, and misused identity, where a person, subject to an alert in SIS, uses the identity of another real person.

³⁵⁵ Article 27(5) of the IO Regulations.

³⁵⁶ Indeed, if a person is known under several identities within a sole IT system, only one link has to be generated with the data eventually present in the other IT system.

³⁵⁷ Article 28(7) of the IO Regulations establishes that the procedure is laid down by the European Commission with an implementing act together with eu-LISA.

³⁵⁸ Article 4(18) of the IO Regulations establish that match ‘means the existence of a correspondence as a result of an automated comparison between personal data recorded or being recorded in an information system or database’.

³⁵⁹ European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 58.

³⁶⁰ According to Article 28(5) of the IO Regulations, the definition of same or similar data should be concretised by the European Commission in a delegated act. This is enabled by an algorithm programmed to detect the similarity between identity data from data fields belonging to different systems. The algorithm would point out when the identity data can be considered similar according to thresholds of similarity previously defined – see the Formal comments of the EDPS on *the draft Commission Delegated Regulations supplementing Regulation (EU) 2019/817 and Regulation (EU) 2019/818 of the European Parliament and Council with regard to cases where identity data may be considered as same or similar for the purpose of the multiple identity detection*, Brussels, 27.04.2021. Although the delegated act has not been published yet, it was objected by the European Parliament that complained about the fact that the European Commission wanted to sub-delegate that power to eu-LISA and to experts from the European Commission, the Member States and the Union agencies ‘using the EU information systems and interoperability components’ – see the European Parliament, *Objection to a delegated act: Determining cases where identity data may be considered as same or similar for the purpose of the multiple identity detection pursuant to Regulation (EU) 2019/817*, P9_TA(2022)0007, Strasbourg, 20 January 2022.

and the templates held by the sBMS belong to the same person. The same or similar identities do not require a 100% match: the former requires that only some data is equal – e.g., the surname and first name; the latter occurs when transliteration errors or inversions of categories of data are detected. Take, for example, the case of a third country national requesting a visa for the first time in a third country. In this case, an individual file will be created in the VIS. Reaching the EU external borders the individual will be registered in the EES, too. In both instances, that is, when a file is created in the VIS and in the EES³⁶¹, the multiple-identity detection procedure is launched. A white link should be generated from the EES file to the VIS one since the two files belong to the same third country national. Provided that the border guard has to manually input the surname (family name), first name or names (given names), date of birth, nationality or nationalities, and gender of the visa holder³⁶², a white link will also be generated in case the authority makes a transliteration error – e.g., if they input “Francesca Tasinari” in the EES, though the consul correctly registered the individual as “Francesca Tassinari” in the VIS. Therefore, white links are definite decisions taken by an Automated Decision-Making (ADM) system in which the human being does not intervene. In our view, this short presentation suggests that within the multiple-identity detection procedure the MID works as machine learning applied to a cloud – the CIR³⁶³:

‘Machine learning is the process by which a computer system trains itself to spot patterns and correlations in (usually large) datasets and to infer information and make predictions based on those patterns and correlations without being specifically programmed to do so’³⁶⁴.

An ADM system may be supervised or not, that is, it may need human intervention to establish the outcomes stemming from the procedure or it may not: ‘where the system is guide or one tool among several for a human decision-maker who ultimately brings their judgement

³⁶¹ Note that in the case of the EES, the situation is quite complex since Article 23 of the EES Regulation establishes that borders authorities shall verify – i.e., a one-to-one comparison – an individual’s facial image or fingerprints with a previous existing file recorded in the EES. Biometric identification, instead, is allowed when: the search with the alphanumeric data indicates that data on the third-country national are not recorded in the EES; where a biometric verification of the third-country national fails, or where there are doubts as to the identity the third-country national. Provided that the MID procedure can be launched only with biometric identification – i.e., one-to-many comparison – the co-legislators should have clarified when the MID is activated in the former (and ordinary) situation.

³⁶² Articles 14(3) and 16(1)(a) of the EES Regulation.

³⁶³ The main characteristics of a cloud are usually resumed by the four “v” that describe the performance of massive (volume) scale of different types of data (variety) in the latest time as possible (velocity) with the highest quality (veracity) – see Rajeev Gupta, Himanshu Gupta, and Mukesh Mohania, “Cloud Computing and Big Data Analytics: What Is New from Databases Perspective?”, in Srinath Srinivasa Vasudha Bhatnagar, *Big Data Analytics. Lecture Notes in Computer Science*, Vol. 7678, Berlin/Heidelberg, Springer, 2012, p. 42, standing out that: ‘[...] clouds are cheap and allow businesses to off-load computing tasks while saving IT costs and resources’.

³⁶⁴ Jennifer Cobbe, “Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making”, *Legal Studies*, Vol. 39, No. 4, 2019, p. 3.

to make the final decision themselves³⁶⁵. In cases where supervised machine learning is required, a training phase is deployed before it is made operational in order to test the dataset provided by ‘the designer’. In other words, it is the human being who chooses the set of data to be matched as well as the outcome pursued as a result of the analysis of that data. The machine in turn, finds patterns and correlations among the data. After this stage, the machine is ‘ready’ to be used: when it is fed with new data, it can make predictions according to the trained model. Such an outcome may be ‘taken for granted’ and used as a final decision or to support an individual in making their own decision. This should not allow the competent authorities to have blind trust in the machine’s outcomes, as Cobbe highlights:

‘[...] reviewers of ADM should be careful not to assume that machines necessarily make better decisions than humans, that machines make decisions which are free from human biases, or that reviewers do not need to exercise the same scrutiny of decisions made by machines as they would of decisions made by humans. ADM systems are engineered by humans, overseen by humans, and used for purposes determined by humans. Training datasets are constructed by humans, and machine learning models are trained to meet a particular standard but not necessarily audited internally or tested across all possible outcomes. As a result, there may be unidentified quirks, flaws, and other problems in the system’s statistical model which in certain circumstances result in faulty decisions’³⁶⁶.

Therefore, the use of ADM may not be the best solution in cases where the competent authority triggering the MID must exercise discretionary powers – as is usually the case in the administrative field – as the machine is unable to break out of predefined patterns³⁶⁷. From our perspective, the fact that the MID works on pre-established links – i.e., outcomes – to which the co-legislators have attributed a specific meaning, suggests that this component can be perceived as a machine learning process trained on the basis of an ADM supervised model to make predictions using the data inserted in the CIR and the sBMS. However, the IO Regulations do not state this, and it remains our personal opinion³⁶⁸. If we are correct, the compatibility of ADMs with the EU data protection *acquis* – namely, Article 22(1) GDPR, Article 11 LED, and Article 24 EUDPR – must be assessed. Recalling Article 22(1) GDPR for which:

³⁶⁵ *Ibid.*, p. 4.

³⁶⁶ *Ibid.*, p. 8.

³⁶⁷ *Ibid.*, p. 20: ‘[...] machine learning systems may be inappropriate for decisions where discretionary powers are likely to need to be exercised on a case-by-case basis, or in other situations where policy may generally be applied but where exceptions are likely to need to be permitted’.

³⁶⁸ The European Parliament resolution of 12 February 2020 on automated decision-making processes: ensuring consumer protection and free movement of goods and services (2019/2915(RSP)), *OJ C* 294, 23.7.2021, pp. 14-17, was adopted on the occasion of the EU strategy on AI proposed on the 19 February 2021. As the “Intelligence artificielle, les eurodéputés souhaitent une approche fondée sur le risqué”, *Bulletin Quotidien Europe*, No. 12410, 24.1.2020, reports, claims: ‘[...] algorithms must be unbiased and data sets must be unbiased and of high quality. He further advocates that the European citizen should be informed about how an algorithm works, how decisions can be checked and corrected, and whether prices have been customized’ (our own translation).

‘The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her’.

According to the GDPR, the right not to be subjected to ADM can be derogated if the decision is:

- necessary for the entering into, or the performance of, a contract between the data subject and a data controller;
- authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, or
- based on the data subject's explicit consent.

While the first and last points introduce major guarantees to ADM, the second one, which concerns the public sector, means that the national or Union law to which the controller is subject must lay down ‘suitable measures to safeguard the data subject's rights and freedoms and legitimate interests’³⁶⁹. Moreover, Article 22(3) GDPR prohibits individual ADM based on special categories of personal data – including biometrics³⁷⁰ – except when one of the following circumstances apply:

- the data subject gave explicit consent to the processing of their personal data for one or more specified purposes, or
- the ‘processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject’³⁷¹.

Therefore, individual full ADMs based on biometric data derogate the exception to the general rule: even if individual full ADMs are prohibited, and even if the processing of special categories of personal data is forbidden, both rules are derogated by virtue of a law whose norms pursue an objective covered by ‘reasons of substantial public interest’. Such a dual prohibition indicates that the MID deals with extremely delicate data processing activities, the limits to which must be found in the principle of proportionality according to the objective pursued and in respect of the essence of the right to the protection of personal data – namely Article 52(1) of the CFREU³⁷². We believe that the co-legislators should have laid down adequate and

³⁶⁹ Article 22(2)(b) GDPR.

³⁷⁰ Article 9(1) GDPR.

³⁷¹ Article 9(2), (a) or (g) GDPR.

³⁷² Articles 7, 8 and 52(1) of the CFREU.

specific measures regarding the multiple-identity detection procedure to protect the interests and fundamental rights of the data subject.

Clearer are the guarantees foreseen by the LED, Article 11 of which sets forth that the ADM prohibition concerns only automated processing that ‘produces an adverse legal effect concerning the data subject or significantly affects him or her’, unless it is established by Union or Member States’ law to which the data controller is subject and ‘appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller’ are in place. Therefore, the adoption of individual full ADM is allowed in cases where ‘legal effects’ on the data subject occur. In cases of ‘adverse legal effects’ or of ‘significant affectation’ it will be sufficient to comply with the principle of legality to lift up the general prohibition. Moreover, in these cases, the use of ‘special categories’ of personal data is permitted ‘unless suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests are in place’³⁷³. In other words, there is no the need to claim an ‘essential reason of public interest’.

The different regulations set forth in the GDPR and the LED are of paramount importance as they establish different limits on national and EU legislators when it comes to regulating individual fully-automated decisions mechanisms. Provided that a MID-white link generated in a fully automated manner is expected to benefit *bona fide* travellers, it should be deemed to produce ‘legal effects’ regarding them in the light of Article 22(1) GDPR. While it seems not to integrate the parameters of an ‘adverse legal effect’, the exclusion of a ‘significant affectation’ of Article 11(1) LED is far less clear. Therefore, white links would, in principle, be forbidden in light of the GDPR, but probably in the case of the LED. The fact that links are generated within data initially stored for different operational purposes blurs the lines between the legal frameworks applicable to ADM. The same uncertainty occurs when the final decision should be attributed to an EU institution, body, or office, as the EUDPR follows word-for-word the norms of the GDPR and the LED.

The choice of the underlying framework has a crucial impact on: the right to information; the right to access, rectify, and suppress personal data, as well as the right to oppose data processing activities, as the latter was set forth by Article 21 GDPR but not by the LED. Data subjects’ rights aim at safeguarding the fundamental rights to a private life and, most of all, to the protection of personal data sealed under Articles 7 and 8 of the CFREU. Being as they are relative rights that can be derogated in light of Article 52(1) of the CFREU, the choice of the

³⁷³ Article 22(2) LED.

GDPR or the LED affects the assessment on the limits that can be imposed on the exercise of individuals' rights³⁷⁴. The IO Regulations do not provide a clear distinction between these two legislative measures and, in fact, do not address the possibility that white links should be interpreted as ADMs. Therefore, not only it is unclear as to which framework the data subject should refer to while exercising their rights, but the lawfulness of the automated decisions taken by the multiple-identity detection procedure can be ultimately questioned.

As advanced above, in case of unclear identities a yellow link is generated in place of a white link and in an automated manner. Here, the ADM procedure is not able to establish whether the data belongs to the same person or not as there are some discrepancies among biometrics, identity data, and/or travel document data. As a general norm, the ESP notifies the existence of the yellow link to the authority that inputted or modified the file triggering the multiple-identity detection procedure to notify it of the creation of the new record. It must be noted that the circumstances in which yellow links can occur have been pre-established and may occur in four main situations³⁷⁵:

- the linked data shares the same biometric data but has similar or different identity data;
- the linked data has different identity data but share the same travel document data, and at least one of the EU information systems does not contain biometric data on the person concerned;
- the linked data shares the same identity data but has different biometric data, or
- the linked data has similar or different identity data, and shares the same travel document data, but has different biometrics.

Therefore, both white and yellow links are established in an automated manner. Yet, these links are not a cause of great concern from a legal perspective: yellow links are “provisional” and support the activity of the competent authorities in charge of taking the final decision while resolving them³⁷⁶. A yellow link would be generated, for example³⁷⁷, if a third country national has an alert on refusal of entry in the SIS, in which dactyloscopic data and facial images are stored. If s/he the subject obtains a genuine passport of another country that is subject to visa requirements for entering the Schengen area, at the moment in which the visa is requested, the consular authority will enter the data in the VIS which launches the multiple-identity detection

³⁷⁴ See Chapter I.

³⁷⁵ Article 30(1) of the IO Regulations.

³⁷⁶ Which excludes the application of Article 22 GDPR and Article 11 LED – see Jon Kleinberg, Himabindu Lakkaraju, Jure Leskovec, Jens Ludwig, and Sendhil Mullainathan, “Human decisions and machine predictions”, *The Quarterly Journal of Economics*, 2018, pp. 237-293.

³⁷⁷ See Article 30 of the IO Regulations.

procedure. The sBMS will find that the biometrics correspond to the SIS alert and the MID will create a yellow link as the alphanumeric data and travel document data differ. From this moment on, the procedure is “humanised” and shifts to the manual verification stage.

ii) The manual verification procedure: The resolution of yellow links

As its label suggests, the “manual verification” procedure calls for human intervention³⁷⁸. As a general rule, the authority responsible for resolving a yellow link is the same one that created or modified the file in one of the underlying IT systems³⁷⁹ – i.e., a Member State’s competent authority³⁸⁰ – and this must be reflected in the identity confirmation file stored in the MID³⁸¹. Several authorities are involved in this stage:

- border guards, competent visa authorities, and immigration authorities for the EES;
- visa authorities and authorities competent for the issuance for residence permits as far as the “new VIS” is concerned;
- the ETIAS Central Unit and ETIAS National United for ETIAS;
- the SIRENE bureau of the Member State that creates or updates a SIS alert, and
- the central authorities of the convicted Member State competent for entering data in ECRIS-TCN³⁸².

Conversely, Union agencies cannot enter or modify files in the underlying systems or the CIR and their staff is not competent to conduct a manual verification procedure, as a general rule³⁸³. An important exception is made in cases where the link involves one or more SIS

³⁷⁸ Article 29 of the IO Regulations.

³⁷⁹ Article 29 of the IO Regulations.

³⁸⁰ European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 32. Therefore, Member States discarded the possibility to establish a Central Link Verification Unit (CLV unit) in charge of resolving all the links alone or together with the Member States with the exception of the ETIAS Central Unit in the terms analysed below.

³⁸¹ See *supra*. Article 71(1) of Regulation (EU) 2019/817 and Article 67 of Regulation (EU) 2019/818 establish that the national authorities using or accessing the MID and the CIR are notified to eu-LISA that must publish – and update – a list on the *OJ* three months from the date on which each interoperability component commenced operations. The European Commission, then, is in charge of notifying the Member States and the public through the website

³⁸² Article 26(1) of the IO Regulations. Note that the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) - Presidency revised text of provisions specific to this Regulation*, 6551/18, Brussels, 28 February 2018, p. 9 and 12, contemplated also: the authorities competent to assess a request for international protection provided for in the Eurodac Regulation when assessing a new request for international protection; the authorities competent to collect the data of a third country national or stateless person apprehended in connection with the irregular crossing of an external border provided for in the Eurodac Regulation when creating or updating data in the Eurodac, and the authorities competent to collect the data of a third country national or stateless person found illegally staying in a Member State provided for in the Eurodac Regulation when creating or updating data in the Eurodac.

³⁸³ In Chapter VI, we will see that the possibility for Europol to directly insert alerts in the SIS has been definitely discarded.

“sensitive alert” according to Regulation (EU) 2018/1862, when dealing with the following categories of individuals:

- persons wanted for arrest for surrender or the extradition purposes referred to in Article 26 of Regulation (EU) 2018/1862;
- missing or vulnerable persons referred to in Article 32 of Regulation (EU) 2018/1862;
- persons sought to assist in a judicial procedure referred to in Article 34 of Regulation (EU) 2018/1862, and
- persons that are sought for discreet checks, inquiry checks or specific checks referred to in Article 36 of Regulation (EU) 2018/1862.

In these cases, the authority competent for the manual verification is always the SIRENE Bureau of the Member State that created the alert³⁸⁴. The IO Regulations do not clarify how the SIRENE Bureau is called on to resolve the link, yet the European Commission Delegated Act on linking data specifies that a MID SIRENE mailbox will be established to send a form to the competent SIRENE Bureau. The form will include the information necessary to analyse the link, including the personal data linked by the multiple-identity detection procedure.

As we anticipated, the resolution of yellow links creates new access rights directed at assessing the different identities in question and at adding new coloured links to the identity confirmation file. Specifically, the resolution of yellow links allows the verifying authority responsible for the manual verification procedure to access the ‘linked data contained in the relevant identity confirmation file and to the identity data linked in the CIR and, where relevant, in SIS’³⁸⁵. This assumption is ambiguous as it implies that the identity confirmation file, that is stored in the MID, contains the data and not the links. It also suggests that the links are stored in the CIR and in the SIS, and not in the MID. In practice, to resolve a yellow link the competent authority will have access to the two sets of linked data stored in the CIR and, in case of updating an existing file, to the links already stored in the MID. The fact that the IO Regulations instead refer to ‘link data’, confirms our assumption that links are regarded as personal data in the terms of the EU data protection *acquis*, the consequences of which will be addressed shortly.

All in all, the verifying authority must turn the yellow link into a white, green, or red one. In the words of the IO Regulations:

- a white link is established if the authority competent for the manual verification considers that the data belongs to the same person;

³⁸⁴ Article 29(2) of the IO Regulations.

³⁸⁵ Article 29(3) of the IO Regulations.

- a green link is established if the authority competent for the manual verification procedure considers that the data belongs to two different persons that have similar identities, and
- a red link refers to a person using different identities in an unjustified manner, or a person using someone else's identity in an unjustified manner.

The fact that the IO Regulations insert a new procedure for detecting multiple identities that is triggered each time an individual file is inserted or modified in one of the six large-scale IT systems justifies the concerns that surround the manual verification procedure in terms of the efficiency of the individual checks carried out at the external borders³⁸⁶. In the future, it is envisaged that third country nationals arriving at the EU external borders will normally possess a visa or a travel authorisation issued by the third country of origin³⁸⁷. The multiple-identity detection will be launched in parallel with the EES and SIS one-to-one verification – i.e., to achieve the comparison of biometrics against the individual file created in the EES or SIS respectively. On closer inspection, the resolution of yellow links will require more time than the process already used to execute checks on persons at the external borders³⁸⁸. Regulation (EU) 2019/817 establishes that in cases where the authority responsible for the manual verification procedure is the one creating or modifying a file in the EES, the verification:

‘[...] shall be initiated in the presence of the person concerned, who shall be offered the opportunity to explain the circumstances to the authority responsible, which shall take those explanations into account’,³⁸⁹ but at the same time ‘it shall take place within 12 hours from the creation of a yellow link’³⁹⁰.

Because of the need and desire to not create delays at the border crossing points, especially the land ones, the co-legislators imposed upon the border guards a deadline, albeit it with a certain level of flexibility, for resolving the yellow links, but they warn that the person concerned must be present. These circumstances give rise to at least two concerns: first, the possibility that the competent authority does accurately not evaluate the link while attempting to process the individual quickly; second, the creation of queues at the external borders – especially at second line checks – which is precisely what the co-legislators sought to avoid, as

³⁸⁶ Article 29(4) of Regulation (EU) 2019/817 that does not figure in Article 29 of Regulation (EU) 2019/818.

³⁸⁷ Possible cases foreseeable for a yellow link to be generated at the borders are those where a new file is created in the EES and links are generated with the other IT systems: the possibility for a person to apply for either visa or travel authorisation at the border, prior to border check; a legitimate change in the situation of the person (e.g. passport change) in between the obtention of a travel authorisation and arrival at border, or fraud attempt after the obtention of a travel authorisation or a visa (e.g. using the passport of another person, who has lawfully obtained a visa or a travel authorisation).

³⁸⁸ Article 8 of the Schengen Borders Code.

³⁸⁹ Article 29(4) of the IO Regulations.

³⁹⁰ Article 29(4), third paragraph, of the IO Regulations.

the rapid crossing of the external borders for *bona fide* travellers was one of the goals pursued by the multiple-identity detection procedure.

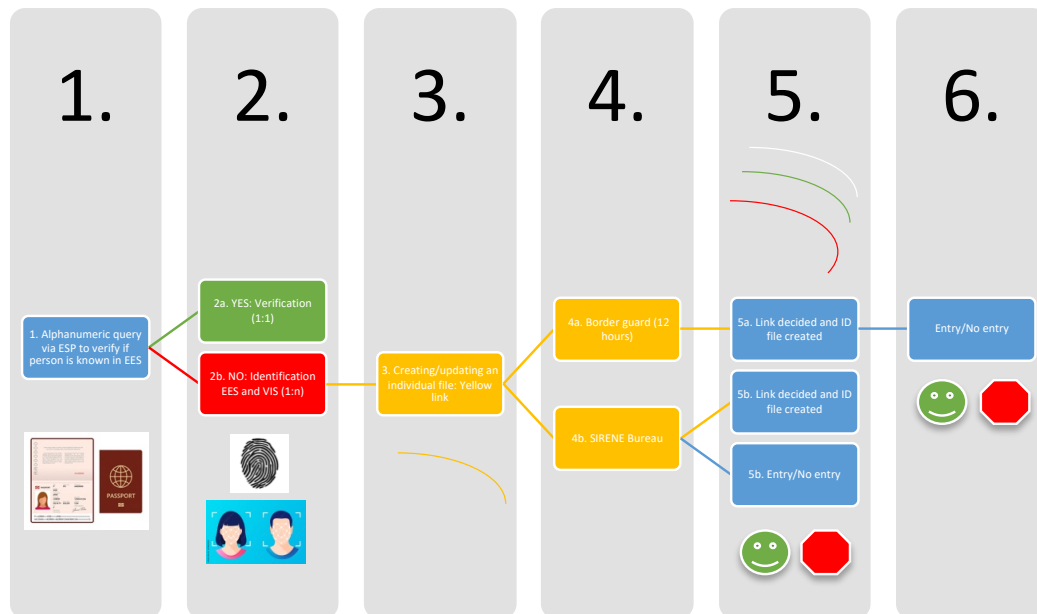


Figure 9 Border check EES process - Source: Own elaboration, images from stock.adobe.com.

In addition, when the IO Regulations were adopted, the co-legislators did not clarify whether the affected person should be aware of the existence of a yellow link to be resolved if their knowing would be detrimental to police and criminal judicial cooperation. This is actually the case of discreet checks for which SIS alerts about ongoing investigations are entered³⁹¹ and, generally speaking, also in cases of so-called SIS sensitive alerts³⁹². In such cases where, on the one hand, the data subject should be not notified of the existence of a link and, on the other hand, where they may pose a threat to the internal security of the EU, no solution has been envisaged. According to the IO Regulations:

‘The authority collecting the personal data to be stored in the shared BMS, the CIR or the MID shall provide the persons whose data are collected with the information required under Articles 13 and 14 of Regulation (EU) 2016/679, Articles 12 and 13 of Directive (EU) 2016/680 and Articles 15 and 16 of Regulation (EU) 2018/1725. The authority shall provide the information at the time that such data are collected’³⁹³.

Therefore, the exemption from sharing information on these links is already embedded in the GDPR and the LED³⁹⁴. Furthermore, as the SIRENE Bureau is the authority competent for resolving the yellow link stemming from a sensitive alert, it is not clear whether the authority

³⁹¹ Article 29(4), third paragraph, of the IO Regulations.

³⁹² See *supra*.

³⁹³ Article 47(1) of the IO Regulations.

³⁹⁴ Article 23(1) GDPR and 13(3)(b) LED.

competent for resolving the link should be notified at its creation. From our perspective, neither should the individual be informed of the link created, in order to safeguard the underlying police investigations³⁹⁵, nor should the border guard be notified provided that they have no competence to resolve it³⁹⁶. For example, in cases where a third country national has an alert for discreet checks in the SIS – including fingerprints and facial imagery – and they then apply for a visa with other identity data, the application would be registered in the VIS – with fingerprints and facial imagery – this launches the multiple-identity detection procedure. The sBMS would find a match against the SIS discreet check alert, but the existence of different identity data would generate a yellow link. While the SIRENE Bureau of the Member State that created the discreet check alert should receive the yellow link notification in order to initiate the manual verification procedure, the visa authority should receive the acknowledgment of the creation of the VIS application and continue the procedure without receiving any information on the match that generated the yellow link.

The IO Regulations suggest that a white, green, or red link should be established by the authority competent for the manual verification according to the following system:

- a white link is established when the files are deemed to belong to the same person³⁹⁷;
- a green link indicates that the files belong to different persons whose identities have some data in common³⁹⁸, and
- a red link is established to signal that there is a high risk that the person is using a different identity in an unlawful manner, it being stolen or false³⁹⁹.

Each coloured link responds to different cases an authority, or an official may have to deal with.

A green link should be established by the authority responsible for the manual verification when they conclude that the data refers to two different persons, in one of the following situations:

- the linked data has different biometric data but shares the same identity data;
- the linked data has different biometric data, has similar or different identity data, and shares the same travel document data;

³⁹⁵ Article 13(3) DPD, see *infra*.

³⁹⁶ Recalling that ‘consulting’ of personal is a data processing activity by virtue of Article 4(2) GDPR. Therefore, access by the border authority to the yellow lines would be an unnecessary processing activity under Article 5(1)(c) of the same Regulation.

³⁹⁷ Article 33 of the IO Regulations.

³⁹⁸ Article 31 of the IO Regulations.

³⁹⁹ Article 32 of the IO Regulations.

- the linked data has different identity data but shares the same travel document data, and at least one of the EU information systems does not contain biometric data on the person concerned.

For example, if a third country national— e.g., Donald Trump – has a SIS alert issued on refusal of entry, and another third country national with the same name and surname – e.g., Trump Donald – asks for an entry visa. In this case, a yellow link would be generated between the VIS and the SIS files. We would expect the link to be converted into a green one as the files belong to two different persons, which the authority should understand by the fact that biometrics do not match. In these terms, the MID will enable the detection of “false positives”⁴⁰⁰, that is cases in which a biometric match erroneously occurs. Once the green link is established, it must be considered as a historical recording established following the MID manual verification procedure. Therefore, green links will be visible to the authorities with access to the two underlying IT systems between which the link is established in case where a “match”⁴⁰¹ occurs between the two sets of linked data. That is, when some of the input data matches with sets of linked data belonging to different persons.

‘This would help avoid, for example, that persons with a name similar to that of a wanted person need to undergo second line border checks each time they cross borders’⁴⁰².

⁴⁰⁰ Note that the IO Regulations do not contemplate cases of false negatives that according to the international standards of the ISO/IEC, *Information technology — Vocabulary — Part 37: Biometrics*, 2382-37, 2017, are ‘[...] of rejecting a biometric claim that should have been accepted in accordance with an authorities statement on the origin of the biometric probe and the biometric reference’. However, it seems to us that in the implementing decision that the European Commission is expected to adopt by virtue of Article 28(7) of the IO Regulations, false negatives were taken into account. According to the EDPS, the European Commission focused to regulate other types of links, that is, the erroneous, the false rejections, and the false acceptance ones, though it had not been empowered to regulate other types of links than the one foreseen in the IO Regulations. The EDPS then questioned whether the act should be underpinned by Article 290 TFEU rather than Article 291 TFEU. Thus, the EDPS suggested using “*flags*” instead of links to highlight the existence of errors – see the Formal comments of the EDPS on the draft Commission Implementing Decisions laying down the technical rules for creating links between data from different EU information systems pursuant to Article 28(7) of Regulation (EU) 2019/817 and Article 28(7) of Regulation (EU) 2019/818 of the European Parliament and of the Council, Brussels, 17.04.2021. Article 32(2), *in fine*, of the IO Regulations establishes that: ‘No legal consequence for the person concerned shall derive solely from the existence of a red link’.

⁴⁰¹ Article 4(18) of the IO Regulations establishes that ‘match’ means ‘the existence of a correspondence as a result of an automated comparison between personal data recorded or being recorded in an information system or database’.

⁴⁰² European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 54.

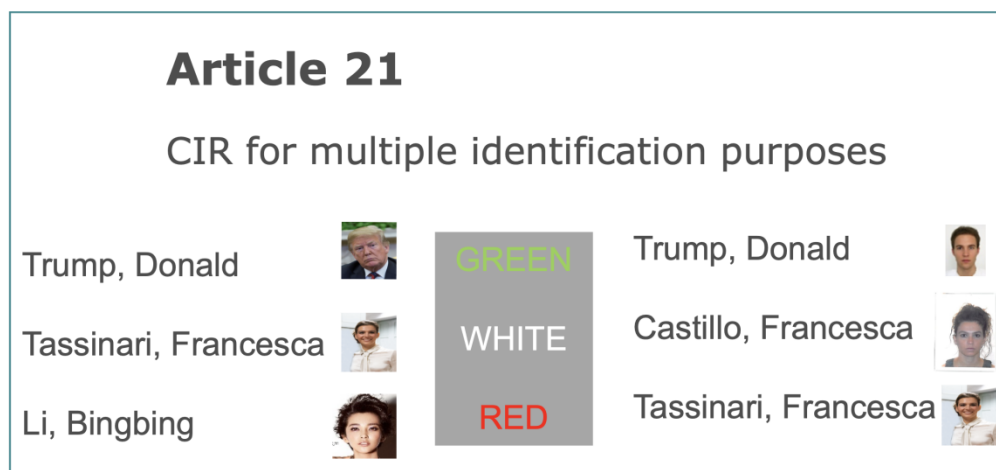


Figure 10 The manual verification procedure – Source: Own elaboration from the author's time working at the European Commission.

Red links should be established by the competent authority in charge of the manual verification procedure when they consider that there are grounds to suspect that: different identities are being used by the same person in an unjustified manner (false identities), or that two different persons are using the same or similar biographical identities in an unjustified manner (identity fraud)⁴⁰³. According to the IO Regulations, red links occur in one of the following circumstances:

- the linked data shares the same biometric data but has similar or different identity data and the authority responsible for the manual verification of the different identities has concluded that the linked data refers to the same person who is using the identity in an unjustified manner;
- the linked data has the same, similar, or different identity data and the same travel document data, but different biometric data and the authority responsible for the manual verification of different identities has concluded that the linked data refers to two different persons, at least one of whom is using the same travel document in an unjustified manner;
- the linked data shares the same identity data, but has different biometric data and different, or no travel document data and the authority responsible for the manual verification of the different identities has concluded that the linked data refers to two different persons acting in an unjustified manner, and
- the linked data has different identity data, but shares the same travel document data, at least one of the EU information systems does not contain biometric data on the

⁴⁰³ Article 32(1)(d) of the IO Regulations.

person concerned and the authority responsible for the manual verification of the different identities has concluded that the linked data refers to the same person, who is acting in an unjustified manner.

Consider, for example, a third country national arriving at the EU external borders from a visa-exempt third country. The migrant has a refusal of entry alert in the SIS, and they have submitted stolen or false data in the ETIAS application to enter the EU. As soon as biometrics are crossmatched between the EES and the SIS, the MID will detect that the person has an alert in the SIS and, consequently, the person is found to have unlawfully declared stolen or false data. Similarly, we may think of a third country national – e.g., Francesca Tassinari – who is known in the SIS and another – e.g., Li Bingbing – who is known in the ECRIS-TCN. Provided that Francesca Tassinari and Li Bingbing have the same biometrics, they would be found to be the same person unlawfully using different identities.

Authorities responsible for the linked data are notified of the creation for a red link – that is, the authorities responsible for the pre-existing data against which a red link has been established – in an automated manner⁴⁰⁴. The consequences deriving from the establishment of a red link must be laid down by EU or national law, though the IO Regulations specify that no legal consequence can be derived from the mere existence of such a link. If the link suggests that identity fraud has occurred, red links are always visible to authorities and EU agencies that have access to the identity data of one of the two systems storing the linked data⁴⁰⁵. Therefore, together with the link, these authorities and EU agencies are allowed to see the references to the EU information systems in which the linked data are held⁴⁰⁶, notwithstanding the fact that the authority competent for the manual verification procedure has access to the corresponding individual file. The rationale underlying the establishment of new access rights is the support function assigned to red links in PJCCM. Indeed, identity fraud and false identities are usually prodromic of the commission of further infractions or crimes and identity fraud is common among organised criminal groups, terrorists, and migrant smugglers in order for them to access the Schengen area unnoticed. Automated solutions are believed to be the most efficient and reliable tools to combat the latest identity fraud techniques⁴⁰⁷ and interoperability bring

⁴⁰⁴ Article 32(6) of the IO Regulations.

⁴⁰⁵ Article 32(2) of the IO Regulations. The authorities accessing the CIR should be notified by the Member States to eu-LISA according to Article 71(1) of Regulation (EU) 2019/817 and Article 67(1) of Regulation (EU) 2019/818 for their publication in the *OJ* within a period of three months from the date on which each interoperability component commenced operations.

⁴⁰⁶ See Article 31(a) and (b) of the IO Regulations.

⁴⁰⁷ The MID speaks about “automatic” rather than automated process. Training is not an efficient tool to detect morphos ‘[i]nstead, computer algorithms may be a better method for minimizing the frequency with which face morphing attacks are missed’, according to Robin S. S. Kramer, Michael O. Mireku, Tessa R. Flack, and Kay L.

important advances in the combating of crimes and the protection of victims. Nevertheless, we must highlight the fact that the establishment of a red link does not show whether the linked data belongs to the fraudster or the victim – i.e., the individual whose identity has been stolen. It is likely that the insertion of a flagging mechanism highlighting when the authority is dealing with a case of false or stolen identity would have helped the authority in identifying cases where they face the victim and not the fraudster. A communication channel to quickly contact the authority that established the red link would have also been reassuring. Another authority or EU agency discovering a red link may wonder whether they should take any action or not, and the authority having established the red link could provide useful information on the circumstances surrounding the case.

In any case, the authorities and staff in question should be instructed to acknowledge that red links must never lead to hasty conclusions. Indeed, when a false or stolen identity is used to illegally access a Member State's territory, then, the holder may be entitled to claim asylum. The use of another individual's identity, or a false one, to access the Schengen area clearly breaks the rules surrounding the lawful entrance to the territory of the Member States: the possession of a valid travel document, including a valid visa permission if held, is a requisite to enter the Schengen area according to the Schengen Borders Code⁴⁰⁸. The CJEU has already ruled that multimodal biometric verification and identification – which includes the use of two fingerprints and a facial image⁴⁰⁹ – are required to combat the use of false identity and identity

Ritchie, *loc. cit.* Other important actions consist in the improvement of the security features of travel documents on which topic the latest Commission Implementing Decision, laying down the technical specifications regarding the standards for security features and biometrics in passports and travel documents issued by Member States and repealing Decisions C(2006) 2909 and C(2008) 8657, C(2018) 7774 final, Brussels, 30.11.2018 and, especially, its Annex.

⁴⁰⁸ See Article 6(1)(a) and (b) of the Schengen Borders Code. In order to assess the compliance of third country nationals with the requirements listed under Article 8 of the Schengen Borders Code, border guards shall consult the relevant databases at their entrance and exit: the VIS for visa holder; the SIS for preventing the entry of persons upon which it is pending a refusal of entry alert; the EES to calculate the duration of the authorised stay of third country nationals; the ETIAS system that inserts a mechanism of automated checks for visa exempt third country nationals. Furthermore, border guards shall consult the relevant databases on stolen, misappropriated, lost and invalidated documents, such as Interpol databases or national ones in the terms we will analyse later on.

⁴⁰⁹ See C-291/12, *Michael Schwarz v Stadt Bochum*, where Mr Schwarz applied for a German passport but refused to have his fingerprints taken and stored in his new passport. The Stadt Bochum rejected his application and Mr Schwarz challenged the validity of Article 1(2) of Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, *OJ* 2004 L 385, p. 1, in the light of Articles 7 and 8 of the CFREU. Also, in C-225/12, *Demir*, 7 November 2013, EU:C:2013:725, para. 41, the CJEU confirmed that '[...] the objective of preventing unlawful entry and residence constitutes an overriding reason in the public interest, it is important too that the measure at issue should be suitable for securing the attainment of that objective and that it does not go beyond what is necessary in order to attain it'. Here, the Court dismissed The Netherlands' petition on whether the standstill clause of Decision 1/80 of the Agreement establishing an Association between the European Economic Community and Turkey, signed at Ankara on 12 September 1963 by the Republic of Turkey, of the one part, and by the Member States of the EEC and the Community, of the other part, and concluded, approved and confirmed on behalf of the Community by Council Decision 64/732/EEC of 23 December 1963, *OJ* 1973, C 113, p. 1, could have been disapplied when more

fraud and, lastly, the illegal entrance of third country nationals⁴¹⁰. This assumption is corroborated by the existence of an explicit EU competence that allows the EU to adopt measures on checks to which persons crossing external borders are subjected – namely, Article 79(2)(c) TFEU. However, the CJEU has never ruled on the necessity and proportionality of the processing of different categories of biometrics of personal data in centralised databases for identification purposes⁴¹¹. Identity checks are *a condicio sine qua non* the person complies with the requirements to enter and exit the Schengen area, as the Schengen Borders Code regulates⁴¹²:

‘All persons shall undergo a minimum check in order to establish their identities on the basis of the production or presentation of their travel documents. Such a minimum check shall consist of a rapid and straightforward verification, where appropriate by using technical devices and by consulting, in the relevant databases, information exclusively on stolen, misappropriated, lost and invalidated documents, of the validity of the document authorising the legitimate holder to cross the border and of the presence of signs of falsification or counterfeiting’⁴¹³.

The CJEU recognised that identity checks regulated by the Schengen Borders Code also have a preventive function for security reasons underpinned by Article 77(2)(b) TFEU. In these terms, multiple-identity detection will facilitate validating the requisites to gain access to, and stay within, the Schengen area. In *A v Migrationsverket*, the Administrative Court for Immigration Matters of Sweden asked whether the identity of a third country national requesting a renewal of his residence permit for family reunification purposes should have been ascertained beyond doubt in order to process the request, even though the third country national was already domiciled in the Swedish territory⁴¹⁴. In this case, the applicant was found to be detained in Norway and to have used a number of false identities. Because of the custodial sentence imposed for the possession and sale of narcotic drugs, the applicant also had a refusal

stringent rules are imposed in order to prevent unlawful entry and residence at the moment of first admission into the territory of a Member State and before an application for a residence permit is made.

⁴¹⁰ The infringement of national norms for entering to and staying in the territory of a Member States might be punished by administrative or criminal law depending on the Member States legislation. In any case, these infringements cannot *a priori* be considered as threatened to national security or public order. According to the CJEU, the evaluation shall be conducted on a case-by-case basis and only when the infringement can affect the fundamental interests of society, then, it can also integrate a public security or a public interest threat.

⁴¹¹ C-291/12, *Michael Schwarz v Stadt Bochum*, and C-446/12 to C-449/12, *W.P. Willems v Burgemeester van Nuth and H.J. Kooistra v Burgemeester van Skarsterlân and M. Roest v Burgemeester van Amsterdam and L.J.A. van Luijk v Burgemeester van Den Haag*, 16 April 2015, EU:C:2015:238. In the latter case, the applicants expressly alleged that the insertion of biometrics in their document constituted *per se* a serious interference and that this was aggravated by the fact that the data would be stored in decentralised databases that, in the future, may have converged in a centralised one. The CJEU affirmed that the conservation of biometrics in decentralised or centralised databases was not regulated by EU law but by national provisions; hence, the latter question should have been addressed to the national judge.

⁴¹² See Article 2(11) of the Schengen Borders Code.

⁴¹³ See Article 8(2) of the Schengen Borders Code.

⁴¹⁴ C-193/19, *A v Migrationsverket*, 4 March 2021, EU:C:2021:168.

of entry alert submitted by Norway. At the same time, Sweden received another application with the same identity data for a resident permit that was rejected for reasons of a marriage of convenience. Hence, the establishment of the identity in light of the Convention implementing the Schengen Agreement⁴¹⁵ and the Schengen Borders Code, including the possession of a valid passport, should have been clarified in order to grant access to the Swedish territory while allowing the individual to stay. In other words, the CJEU analysed whether the national law providing for the issuing, extension, or renewal of a residence permit for family reunification reasons to a third country national staying within the national territory, with a pending refusal of entry alert entered in the SIS by another Member State and without a certain identity established by means of travel document, was compatible or not with the Convention implementing the Schengen Agreement and the Schengen Borders Code.

The CJEU found that although the SIS should be systematically consulted under Article 25(1) of the Convention implementing the Schengen Agreement, a Member State can issue, extend, or renew a residence permit for “substantial reasons” even though the applicant is subject to a refusal of entry alert entered by another Member State. In light of the principle of sincere cooperation⁴¹⁶ Member States are required to consult each other before issuing such permits to suppress the relevant alert and to avoid inconsistencies. On the contrary, the conditions of entry into the Member States’ territories are set forth under the Schengen Borders Code that demands the possession of a valid travel document to cross the border and for a short stay within the territory⁴¹⁷. As Advocate General De La Tour highlighted, in the case of migration, identification acquires an added value when checking the requisites for the entry of third country nationals⁴¹⁸. However, since this was not the case in the example submitted to the Court – i.e., the third country national was already present within the Swedish territory – the CJEU did not look into evaluating whether an ascertained identity constitutes a prerequisite for the entry into a Member State’s territory or not⁴¹⁹. In any case, if the individual crossing the border is an asylum applicant, the situation is more delicate, as the border guard’s decision to not allow their entry based, *inter alia*, on the existence of a red link may prevent them from reaching EU territory or, even worse, it might breach the *non-refoulement* principle when their asylum application is refused in their presence. Specifically, red links *per se* should lead the authority neither to allege the existence of a public policy or internal security concern, nor to

⁴¹⁵ See Article 25(1) of the Convention implementing the Schengen Agreement.

⁴¹⁶ Article 4(3) TEU.

⁴¹⁷ Article 6(1)(a) of the Schengen Borders Code.

⁴¹⁸ Opinion Advocate General De La Tour, C-193/19, *A v Migrationsverket*, 16 July 2020, EU:C:2020:594.

⁴¹⁹ Note that the Schengen Borders Code does not contemplate identification within the requisites to enter the Schengen area.

assimilate its effect into a SIS alert on refusal of entry⁴²⁰. Although the IO Regulations highlight that particular attention should be paid to persons in need of international protection, they do not refer to the *non-refoulement* principle, which would have been preferable in order to ensure the fulfilment of such a vital principle of International human rights law.

Last but not least, a yellow link should be turned into a white link when⁴²¹:

- the linked data shares the same biometric data and the same or similar identity data;
- the linked data shares the same or similar identity data, the same travel document data, and at least one of the EU information systems does not have biometric data on the person concerned;
- the linked data shares the same biometric data, the same travel document data, and similar identity data, or
- the linked data shares the same biometric data but has similar or different identity data and the authority responsible for the manual verification of different identities has concluded that linked data refers to the same person in a justified manner.

If a white link is established, the MID indicates that the identity data corresponds to the same person⁴²², that is, the competent authority is dealing with a person who is lawfully using multiple identities. For example, this could include the case of a person asking for a visa to enter the Schengen area, who changes their surname during the period of time from the issuing of the visa to the checks at the borders⁴²³. At the time of inserting a new file in the EES, the MID would detect that the alphanumeric data was incongruent, so a yellow link would be generated. Also, it may be the case of a woman – e.g., Tassinari Francesca – who changes her surname after marriage – e.g., Castillo Francesca – in which case the linked data would share the same biometric data, the same travel document data, and similar identity data. White links should be also established for third country nationals with dual nationalities who use different travel document data, as their biometrics and identity data are the same. As the FRA underlines⁴²⁴, this implies that the multiple-identity detection procedure will have a major impact on certain categories of persons that will be stopped more frequently at the borders⁴²⁵, as it is the case for people coming from societies that use the same or similar names as a cultural

⁴²⁰ Article 6(1)(e) of the Schengen Borders Code.

⁴²¹ Article 33(1) of the IO Regulations.

⁴²² Article 33(2) of the IO Regulations.

⁴²³ It must be noted that the change of identity could have been taken into account already at the moment of issuing a new visa or authorisation, yet also in this case the EES file should be updated according to the new identity data. The yellow link generated following the update should be turned into a white link between EES and VIS or ETIAS.

⁴²⁴ Council of the EU, *Interoperability and fundamental rights implications*, 8037/18, Brussels, 18 April 2018, p. 14.

⁴²⁵ Elisabeth Hoffberger-Pippan, *loc. cit.*

norm. However, cases of same or similar identity data and different, or no, travel document data cannot generate any link in the absence of biometrics. In addition, the IO Regulations introduce a non-discrimination clause, that according to Prof. Hoffberger-Pippan:

‘By requiring Member States to pay particular attention to such people, the regulation sets an appropriately high standard of protection, which may lead to infringement proceedings before the ECJ in case of non-compliance’⁴²⁶.

In the specific case of the MID, Article 74(6) of the IO Regulations establishes that two years after the start of operations of the MID⁴²⁷ the European Commission should produce an examination of the MID on the right to non-discrimination as a part of the overall evaluation conducted by the European Commission on the achievement of the IO goals. For these purposes, Member States and Europol shall provide eu-LISA and the European Commission with the information necessary to draft the reports without jeopardising any working method, or including information that would reveal the sources, staff members or investigations of the designated authorities. Also, eu-LISA is expected to provide the European Commission with the information necessary to produce the overall evaluation. Although agreeing with Prof. Hoffberger-Pippan’s appreciations on the non-discrimination clause inserted by the IO Regulations, we believe that the launch of an infringement procedure by the European Commission may not be easy to undertake if EU institutions and bodies are not properly informed during the monitoring process. Therefore, it would have been reassuring if eu-LISA were empowered to monitor if the authorities and Union agencies’ staff that are entitled to access the interoperability components actually comply with the IO Regulations, but to do so, Member States would have to give up self-monitoring for an “other-monitoring” procedure⁴²⁸.

White links remain visible to the authority that has access to the two underlying large-scale IT systems. By querying a specific system, this ‘[...] shall reply indicating, where relevant, all the linked data on the person, thereby triggering a match against the data that are linked by the white link, if the authority launching the query has access to the linked data under Union or national law’⁴²⁹. In other words, white links generated in an automated manner or established by the authority competent for the manual verification procedure will be able to allow for the retracing of an individual’s dispersed identity the data of which is lost in different systems. In these terms, the IO Regulations establish that:

⁴²⁶ *Ibid.*, p. 439.

⁴²⁷ See Article 72(4) of the IO Regulations.

⁴²⁸ See further Francesca Tassinari, “La interoperabilidad de los sistemas de información de gran magnitud de la Unión Europea y la detección de identidades múltiples: garantías y responsabilidades”, in Francisco Javier Garrido Carrillo, *Lucha contra la criminalidad organizada y cooperación judicial de la UE: instrumentos, límites y perspectivas en la era digital*, Navarra, Thomson Reuters Aranzadi, 2022, pp. 291-338.

⁴²⁹ Article 33(2) of the IO Regulations.

‘Where a white link is created between data in the EES, VIS, ETIAS, Eurodac or ECRIS-TCN, the individual file stored in the CIR shall be updated in accordance with Article 19(2)’⁴³⁰.

Provided that the SIS II preventive alerts⁴³¹ will support the detection of children who need to be prevented from travelling, and of vulnerable persons of an age needing to be prevented from travelling for their own protection, Article 21 is expected to be very useful in supporting the detection of children in need while consulting other large-scale IT systems like the VIS that collects data on children aged six and older⁴³², or the Eurodac that fingerprints children of at least fourteen years of age⁴³³. All in all, white links can be manually established by the competent authority in cases where they discover that the individual file inserted in one of the underlying systems belong to an existing individual file stored in the CIR⁴³⁴ and that it was not detected by the MID. This would avoid leaving un-linked individual files concerning the same person.

‘Colour-coded’ MID links	Examples
YELLOW Automated generated, yellow links calls for manual verification procedure	Francesca Tassinari (SIS) + Francesca Castillo (VIS) might be the same person
GREEN Same or very similar biographical identities with different biometric data	Donald Trump (SIS) + Donald Trump (VIS) are two different persons
RED Different biographical identities are linked to the same biometric data and manual verification determines that this is unlawful (identity fraud)	Francesca Tassinari (SIS) + Li Bingbing (ECRIS-TCN) is the same person using different identities
WHITE <ul style="list-style-type: none"> - Same biometric data and same (or very similar) biographical data (same person in multiple systems); - Same biometric data but lawfully differing biographical data after manual verification. 	Francesca Tassinari + Francesca Castillo are legally different identities for the same person

Figure 11 Manual verification procedure – Source: Own elaboration.

As a final remark, we would like to highlight that the manual verification procedure may occur in different circumstances that might impact the authority in charge in its resolution of the yellow link. According to the FRA:

‘Significant difficulties also emerged from the so-called hotspots at the EU-supported Greek and Italian processing centres that register and refer newly arrived people. In Italy, officials explained that after a large number of arrivals disembarked, sometimes during the

⁴³⁰ Article 33(3) of the IO Regulations.

⁴³¹ Article 32 of Regulation (EU) 2018/1862.

⁴³² Article 13(7) of the revised VIS Regulation.

⁴³³ Article 9 of the 2013 Eurodac recast Regulation.

⁴³⁴ Article 28(2) of the IO Regulations.

night and after dangerous and long journeys, the police officers in charge of fingerprinting would work in a rush, spending less time explaining the process to individuals⁴³⁵.

The success of the multiple-identity detection procedure depends on the accuracy of the data entered in the underlying systems⁴³⁶, but also on the authority's attention and expertise in enrolling biometric data into a system. Notably, Article 76(1) of Regulation (EU) 2019/817 and Article 72(1) of Regulation (EU) 2019/818 establishes that 'eu-LISA shall perform tasks related to the provision of training on the technical use of the interoperability components in accordance with Regulation (EU) 2018/1726'. Trainings should be organised by the Member States for their authorities and by the Union agencies for their staff in order for them to process data using the interoperability components with special emphasis on data security, data quality, data protection rules, the procedures applicable to data processing, and their obligations to inform the data subject⁴³⁷. In addition, the sister Regulations allow for the setting up of joint training courses organised at the Union level to enhance cooperation and the exchange of best practices between the Member States' authorities and Union agencies' staff who are authorised to process data using the interoperability components. Is not by chance that Article 76 *in fine* of the IO Regulations states that:

'Particular attention shall be paid to the process of multiple-identity detection, including the manual verification of different identities and the accompanying need to maintain appropriate safeguards of fundamental rights'.

b) The multiple-identity detection during the transitional period

The ETIAS Central Unit established within the EBCG Agency has two main tasks: first, it must manually verify multiple identities according to Article 29(1)(c) of the IO Regulations; second, it manages the procedure for the detection of multiple identities in the data established in the EES, the VIS, the Eurodac, and the SIS according to Article 69(1) of Regulation (EU) 2019/817 and Article 65(1) of Regulation (EU) 2019/818⁴³⁸. In both cases, the EBCG Agency must be considered as a 'data controller' according to Article 3, point 8, of the EUDPR with consequences that will be explored later on.

From a preliminary inspection, it is important to highlight that the MID activates a procedure developed in parallel with the automated cross-checks that are launched by the systems and that take place among one another. In the case of the ETIAS, for example, the online submission of a travel authorisation or the specific application triggers a series of automated checks against:

⁴³⁵ FRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Vienna, 2018, p. 32.

⁴³⁶ See *infra*.

⁴³⁷ Articles 32(4), 33(4) and 47 of the IO Regulations.

⁴³⁸ Article 57 of Regulation (EU) 2019/817 and Article 57 of Regulation (EU) 2019/818.

the data stored in the ETIAS; the other IT systems – SIS; VIS; EES; Eurodac; Europol’s data; Interpol’s data stored in SLTD and TDAWN; the ETIAS Watchlist, and the risk criteria for illegal migration, security and public health, which are also known as the screening rules⁴³⁹. If no hit occurs, the travel authorisation is issued in an automated form; if a hit occurs, the ETIAS Central Unit is in charge of verifying if the data hit belongs to the same person. If there is a hit, or there are doubts regarding the identity of the applicant, the ETIAS Central Unit contacts the ETIAS National Unit competent for the manual verification⁴⁴⁰ – this is not so different from the MID procedure. Provided that the submission of a multiple-identity detection procedure is launched in parallel, it is not clear: first, who has to resolve potential yellow links generated among the data entered in the application and in the other systems; and, second, if the generation of a yellow link should impact the procedure of issuing the travel authorisation. We believe that the ETIAS Central Unit should detect the creation of the yellow link as a result of the launching of the multiple identity detection under the framework of the automated procedure regulated by Article 20 of the ETIAS Regulation, notwithstanding the generation of a yellow link or not. If the ETIAS Central Unit confirms the existence of a yellow link, then, the ETIAS National Unit should be notified in order to resolve it. In addition, the procedure to issue an ETIAS authorisation should not be blocked before the generation of a red link, as this cannot constitute the basis of a prejudicial decision – e.g., the individual should not be denied entry into the Schengen area. In other words, the multiple-identity detection procedure should not justify the denegation, annulment, or the revocation of an ETIAS authorisation *per se*⁴⁴¹. These circumstances would break the EU trend in outsourcing⁴⁴² border checks to third countries of origin and transit to remove undesired persons, and it is also useful in the detention of criminals:

⁴³⁹ Articles 12, 20(4), and 33 of the ETIAS Regulation.

⁴⁴⁰ Article 26 of the ETIAS Regulation.

⁴⁴¹ Formal comments of the EDPS on the draft *Commission Implementing Decision laying down standard for refusal, annulment or revocation of a travel authorisation pursuant to Article 38(3) of Regulation (EU) 2018/1240*, Brussels, 25.05.2021.

⁴⁴² José Alejandro del Valle Gálvez, 2002, *op. cit.*, p. 305 ff., and Id., “Control de Fronteras y Unión Europea”, *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid*, No. 7, 2003, pp. 67-92, pp. 72 ff., distinguishes three functions deployed by borders: first, the delimitation of a state’s territorial competences; second, as a place to control the entry and exit of goods and people and, third, as a means for cooperation with neighborhood countries. Early, the author highlighted that there is not a perfect coincidence between border-line and border-place control: ‘So that the states try to develop border controls along the same political-legal lines of the conventionally agreed cut, but it is very frequent that the control of one or another state is not carried out strictly and exactly at one or the other side of the border line’ (p. 307, our own translations). Recently in José Alejandro del Valle Gálvez, “Los refugiados, las fronteras exteriores y la evolución del concepto de frontera internacional”, *Revista de Derecho Comunitario Europeo*, No. 55, 2016, pp. 759-777, p. 774 ff., he observes how the EU is forging a new ‘external border model’ where the border is not a “frontline” but an area where ‘functions of control and access to EU territory, including the processing of asylum applications, the retention of arrivals of refugees or the execution of agreements on the return and return of immigrants and Refugees’ are executed (our own translation).

if the person concerned is wanted, they should be granted the authorisation to enter so that they can be arrested at the borders.

The ETIAS Central Unit will play a central role during the MID transitional period⁴⁴³ when it will have the competence to resolve the yellow links generated from the matching of the legacy data – i.e., that data stored in the large-scale IT systems before the interoperability components enter into operation. The generation and establishment of links during the MID transitional period raise important transparency concerns as the data subject is not informed about the MID, neither at the time when their personal data was collected, nor when the link was generated. The IO Regulations foresee that the resolution of yellow links *vis-à-vis* legacy data must be carried out within a one-year period⁴⁴⁴ from the finalisation of the tests performed on the MID by eu-LISA⁴⁴⁵ to the start of the MID operations, and that this will be done on the basis of biometric data only – which excludes the links generated by ETIAS with EES, VIS, Eurodac and SIS. The multiple identity detection procedure will follow step-by-step the approach analysed above with the specification that the ETIAS Central Unit will have to notify the European Commission as soon as all links have been resolved⁴⁴⁶. The IO Regulations foresee that Member States will support the ETIAS Central Unit to develop this process, but they do not clarify under what terms, or through which channels, such cooperation should be implemented. This legislative gap raises huge concerns as far as the Eurodac is concerned, as this system has not been storing the personal data of asylum seekers and illegal migrants apart from fingerprints and gender. Therefore, cooperation with Member States becomes indispensable in order to resolve the yellow links triggered once the Eurodac has migrated to the CIR. Besides, this system cannot be used in the MID transitional period unless it is reformed as biographical data is needed to make the MID function. Once the MID transitional period is completed, the ETIAS Central Unit must notify the European Commission⁴⁴⁷. Yet, the ETIAS Central Unit cannot resolve the links related to “sensitive alerts”, in these cases the SIRENE Bureau of the Member State creating the alerts is called on to resolve them. Therefore, the SIRENE Bureau is also expected to contribute to the resolution of biometric-based yellow links in the MID transitional period despite the silence of the co-legislators.

⁴⁴³ Article 69 of Regulation (EU) 2019/817 and Article 65 of Regulation (EU) 2019/818.

⁴⁴⁴ The period is renewable for a period of eighteen months – one six-month period, renewable twice for six months each – in accordance with Article 69(8) of Regulation (EU) 2019/817 and Article 65(9) of Regulation (EU) 2019/818.

⁴⁴⁵ Article 72(4), letter (b), of Regulation (EU) 2019/817 and Article 68(4) of Regulation (EU) 2019/818.

⁴⁴⁶ Article 69(6) of Regulation (EU) 2019/817 and Article 65(6) of Regulation (EU) 2019/818.

⁴⁴⁷ Article 69(6) of Regulation (EU) 2019/817 and Article 65(6) of Regulation (EU) 2019/818.

c) The right to information on the links

The automated links generated or established by the multiple-identity detection procedure are ‘[...] information relating to an identified or identifiable natural person’ or, put simply, personal data⁴⁴⁸. The links enable the identification of the data subject to whom the linked data belongs and the references to the data contained in the systems and the CIR are stored in the MID. This also seems to be the position of the co-legislators that set forth enhanced guarantees to protect the links’ data against abuse by national authorities and Union agencies.

Above all, Articles 32(4) and 33(4) of the IO Regulations establish that the person must be informed if the authority competent for the manual verification procedure establishes a white or a red link so as to facilitate the exercise of the right to access, rectify, suppress or restrict the processing of personal data. The right to be informed can be restricted only if the information imperils ‘security and public order, prevent crime and guarantee that no national investigation will be jeopardized’⁴⁴⁹. Specifically, the authority competent for the manual verification procedure must inform the data subject ‘in writing by means of a standard form’⁴⁵⁰. However, the IO Regulations do not define how the form should be administrated when a white/red link is established in the absence of the person – e.g., when a white or a red link is established by the ETIAS Central/National Unit – which infers that, in practice, the individual will not always be informed regarding the establishment of coloured links that concern them.

The adoption of a standard form has been delegated to the European Commission through two implementing decisions – one for Regulation (EU) 2019/817⁴⁵¹ and another for Regulation (EU) 2019/818⁴⁵². In case several links are created, one form will be issued per link. The form will be available in the languages referred to in Article 2(3) of the European Commission Delegated Regulation which lays down detailed rules on the operation of the web portal⁴⁵³. It contains a reference to the single identification number and the contact details for: the Data Protection Officer of the authority responsible for the manual verification of different identities; the EDPS, and the national supervisory or data protection authority. Following the EDPS’

⁴⁴⁸ Articles 4(1) GDPR and LED, and Article 3(1) EUDPR.

⁴⁴⁹ Articles 32(4) and 33(4) of the IO Regulations.

⁴⁵⁰ Articles 32(5) and 33(5) of the IO Regulations.

⁴⁵¹ Article 32(5) and 33(6) of Regulation (EU) 2019/817.

⁴⁵² Article 32(5) and 33(6) of Regulation (EU) 2019/818.

⁴⁵³ Commission Delegated Regulation (EU) 2021/2104 of 19 August 2021 laying down detailed rules on the operation of the web portal, pursuant to Article 49(6) of Regulation (EU) 2019/817 of the European Parliament and of the Council, C/2021/5050, OJ L 429, 1.12.2021, pp. 72-78.

analysis⁴⁵⁴, we can appreciate that the authorities competent for the manual verification procedure can tick one of the four boxes contained in the form to inform the individual of the reason why a white or red link has been established. These boxes cover the following:

- the identity information is not (or not entirely) the same, the biometrics are the same, and the verification process indicates that it is the same person;
- the travel document and possibly the identity information are the same, the biometrics are different, and the verification process indicates that two different individuals are using the same travel document;
- the identity information is the same, the biometrics and possibly the travel document are different, and the verification process indicates that two different individuals are using the same identity, or
- the identity information is different, the travel document data is the same, and the verification process indicate that this is the same person.

The EDPS suggested laying down the possibilities stemming from each case in more detail. Similarly, and with regard to white links, the EDPS recommended substituting the reference to the fact that discrepancies had been detected with regard to the personal information concerning the individual, with other non-technical and comprehensible information. In their words:

‘[...] the verification authorities should indicate the (justified) discrepancies identified or explain at least in abstract terms possible discrepancies between the data stored in different systems and what it means practically that they are deemed justified’⁴⁵⁵.

Surprisingly, the EDPS did not advance the possibility that the individual would not be informed in a free, specific, informed, and unambiguous way in the EU legislation’s terms, especially considering the complexity of the multiple-identity detection procedure in which an ADM mechanism had been introduced. It must be recalled that ADMs based on algorithms – or black boxes – end up watering down the data subject’s right to be informed because of the intrinsic inexplicability of their functioning and, in any case, their technical complexity hampers comprehension on the part of the individual. There are those that maintain that the right to be

⁴⁵⁴ Formal comments of the EDPS on *the draft Commission Implementing Decisions laying down a standard form for notification of a white link pursuant to Regulation (EU) 2019/817 and Regulation (EU) 2019/818 of the European Parliament and of the Council*, Brussels, 22.04.2021, and Formal comments of the EU on *the draft Commission Implementing Decision laying down a standard form for notification of a red link pursuant to Regulation (EU) 2019/817 of the European Parliament and the Council*, Brussels, 31.03.2021.

⁴⁵⁵ Formal comments of the EDPS on *the draft Commission Implementing Decisions laying down a standard form for notification of a white link pursuant to Regulation (EU) 2019/817 and Regulation (EU) 2019/818 of the European Parliament and of the Council*, Brussels, 22.04.2021, and Formal comments of the EU on *the draft Commission Implementing Decision laying down a standard form for notification of a red link pursuant to Regulation (EU) 2019/817 of the European Parliament and the Council*, Brussels, 31.03.2021, p. 3.

informed should be intended as a right to the explication⁴⁵⁶ and those that do not⁴⁵⁷ – this impedes our understanding under what terms the affected person should be granted access to the information on how the ADM functions. Given this, the EU legislator might have taken the first steps to provide clarity regarding this serious issue, given that:

‘The result of algorithmic opacity is that an automated system’s decision-making process may be difficult to understand or impossible to evaluate even for experienced systems designers and engineers’⁴⁵⁸.

The co-legislators might have enhanced the individual right not to be subjected to ADM, highlighting that, despite the supportive function of the machine, the final decision on establishing a white or red link is taken by a (human) competent authority. These guidelines should be translated to the Member States’ authorities too, for example, in the form of the trainings⁴⁵⁹ that are foreseen by the IO Regulations to ensure their harmonised execution.

Another criticism from the EDPS concerns the provision contained in the standard form that states that when a white or red link is established, the individual is not required to undertake any action, but is free to contact the competent authority to receive more information on the linked data. According to the EDPS, this sentence is contradictory, as it subjects the exercise to the right to information and access to personal data to the suspicion that an error has occurred. Therefore, the EDPS suggested deleting the sentence ‘no action of the individual is required’. It seems probably that the European Commission wanted to avoid the possibility that the person exercises their data rights systematically, which would go against the spirit of the EU data protection *acquis*⁴⁶⁰. However, the most transparent solution would be to clearly explain that the links are personal data and, as such, the data subject is the holder of a series of rights exercisable at their discretion. If this were done, the EDPS’ desire to clarify the right to access,

⁴⁵⁶ Troisi Emiliano, “AI e GDPR: L’Automated Decision Making, la Protezione dei Dati e il Diritto alla ‘Intelligibilità’ dell’Algoritmo”, *European Journal of Privacy Law & Technologies*, No. 41, 2019, pp. 41-59; Bryce Goodman and Seth Flaxman, “European Union regulations on algorithmic decision-making and a ‘right to an explanation’”, *2016 ICML Workshop on Human Interpretability in Machine Learning* (WHI 2016), 2016, pp. 1-9; Gianclaudio Malgieri and Giovanni Comandé, “Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation”, *International Data Privacy Law*, Vol. 7, No. 4, 2017, pp. 243-265.

⁴⁵⁷ Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, “Why a right to explanation of automated decision-making does not exist in the GDPR”, *International Data Privacy Law*, No. 2, 2017, pp. 76-99; Andrew D Selbst and Julia Powles, “Meaningful information and the right to explanation”, *International Data Privacy Law*, Vol. 7, No. 4, 2017, pp. 233-242; Lilian Edwards and Michael Veale, “Slave to the Algorithm? Why a ‘Right to an Explanation’ Is Probably Not the Remedy You Are Looking For”, *Duke Law & Technology Review*, 17, 2017, pp. 18-84.

⁴⁵⁸ Jennifer Cobbe, *op. cit.*, p. 5. As Cobbe highlights, three levels of opacity can be inferred from the algorithm-based decisions-making: ‘intentional opacity’ aims at protecting intellectual property; ‘illiterate opacity’ is understandable to those with the technical ability to read and write code, and ‘intrinsic opacity’, where a system’s complex decision-making process is difficult for any human to understand.

⁴⁵⁹ Article 76 of Regulation (EU) 2019/817 and 72 of Regulation (EU) 2019/818.

⁴⁶⁰ Article 12(5) GDPR.

rectify and suppress personal data, as well as the right to restrict data processing activities, would be respected. Conversely, no reference to the right to appeal the decision is provided at this stage, which could leave the individual unsure how to react if the authority responsible for the manual verification does not respond when contacted. The form specifies that the individual should access the web address of the web portal to contact the authority responsible for the manual verification. It also states that the data subject should insert ‘the reference found at the top of this page and the single identification number in any communication’⁴⁶¹. That is, the subject should provide the single identification number and reference number to the authority responsible for the manual verification of multiple identities.

A sensu contrario, from the IO Regulations it is understood that the individual will not be handed-in any standard form when:

- white links are generated in an automated manner, or
- the authority in charge of the manual verification procedure establishes a green link.

These omissions would not deprive the individual of the right to be informed on the processing of his/her personal data *tout court*. As a general norm, the individual must be informed each time a file is created in the SIS, the VIS, the EES, the ETIAS, and the ECRIS-TCN⁴⁶² according to Articles 13 and 14 GDPR, Articles 12 and 13 LED, and Articles 15 and 16 EUDPR. Specifically, this information must be provided when:

- an individual file is created or updated in the SIS in accordance with Article 52 of Regulation (EU) 2019/817 and Article 67(2) of Regulation (EU) 2019/818⁴⁶³;
- an application file is created or updated in VIS in accordance with Article 8 of the VIS revised Regulation;
- an individual file is created or updated in the EES in accordance with Article 14 of the EES Regulation;
- an application file is created or updated in ETIAS in accordance with Article 19 of the ETIAS Regulation, and

⁴⁶¹ Formal comments of the EDPS on the draft Commission Implementing Decisions laying down a standard form for notification of a white link pursuant to Regulation (EU) 2019/817 and Regulation (EU) 2019/818 of the European Parliament and of the Council, Brussels, 22.04.2021, and Formal comments of the EU on the draft Commission Implementing Decision laying down a standard form for notification of a red link pursuant to Regulation (EU) 2019/817 of the European Parliament and the Council, Brussels, 31.03.2021, p. 3.

⁴⁶² Article 47 of the IO Regulations that recalls Articles 13 and 14 GDPR, Articles 12 and 13 DPD, and Articles 15 and 16 EUDPR.

⁴⁶³ Note that Article 47 of Regulation (EU) 2019/818 does not refer to the SIS but we believe that it should have done so.

- the rules on the right to information contained in the applicable Union data protection rules apply to the personal data recorded in ECRIS-TCN.

Therefore, we do not think that ‘an enhanced information for individuals ‘at the stage of collection’ of his/her personal data’ is missing⁴⁶⁴. Provided that the right to information is directed at guaranteeing free, specific, informed, and unequivocal consent regarding the processing of personal data, the IO Regulations predispose some specific guarantees for foreign individuals and children⁴⁶⁵. Indeed, the right to information may be infringed upon in different ways: not only where the information is not ‘spontaneously’ provided, but even worse, in cases of misinformation and unintelligible information being provided. According to the FRA:

‘[...] authorities that collect personal data of asylum and visa applicants, as well as of migrants in an irregular situation, and then store these data in IT systems, find it challenging to provide information in an understandable manner [...] With interoperability, ensuring the right to information may become increasingly challenging’⁴⁶⁶.

National authorities and Union agencies must inform the individual according to the EU *acquis* on the protection of personal data. Nevertheless, it is unclear why the co-legislators have created any forms for cases concerning auto-generated white links and manually verified green links. The creation of a white link in an automated manner and the establishment of a green link following a manual verification procedure produce juridical effects on the individual— i.e., the linking of different personal data. It seems to us that the EU legislator is aware of the impossibility or extreme difficulty in understanding why a machine has taken one decision instead of another. Although at first sight green links do not allow the identification of a unique person, but aim at distinguishing them from another, this type of link contributes to the systematisation and management of cases lost in the different systems that were implemented following the silo approach⁴⁶⁷. Nothing prevents both white and green links being erroneous or illegally stored, which does not explain the different treatment given to the interested person *vis-à-vis* white or red links owners.

⁴⁶⁴ Niovi Vavoula, 2020, *op. cit.*, p. 154.

⁴⁶⁵ Articles 47(2) of the IO Regulations: ‘All information shall be made available, using clear and plain language, in a linguistic version the person concerned understands or is reasonably expected to understand. This shall include providing information in a manner which is appropriate to the age of the data subjects who are minors’.

⁴⁶⁶ FRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Vienna, 2018, p. 9.

⁴⁶⁷ Matthias Leese, *loc. cit.*, points out that the context of interoperability, and especially in the CIR, a new formula for identity management for the governance of the Schengen area is emerging. Since the concept of identity management usually refers more to the authentication of users when accessing IT systems, we believe that it would perhaps be more appropriate to speak of a CMS when approaching the IO Regulations.

d) The right to access, rectify, and erase personal data stored in the Multiple-Identity Detector and the right to restrict the processing of personal data

i) The web portal

As the EDPS highlights, the standard form that the European Commission is working on contains a link to access the web portal⁴⁶⁸. The web portal was proposed⁴⁶⁹ by the European Parliament during the negotiations on the interoperability package to facilitate the rights to access, rectify, suppress, and restrict the processing of personal data⁴⁷⁰. It consists of a publicly available website where the data subject will find: additional details about the MID; the contact details of the authority that created the specific red link, and an example e-mail (template)⁴⁷¹ that they can use to make their request. According to the IO Regulations, the web portal is a ‘user interface enabling persons whose data are processed in the MID and who have been informed of the presence of a red link [...] to receive the contact information of the competent authority of the Member State responsible for the manual verification of different identities’⁴⁷². In other words, the web portal allows the individual to contact the authority competent for the manual verification procedure that turned the yellow link into a white or red one. We should highlight the fact that, from Article 49(2) of the IO Regulations, the web portal seems to only be directed to people for whom a red link has been issued, and not to those people for which a white link had been established following a manual verification. However, since both forms deal with such a link⁴⁷³, it is reasonable to believe that those who have their data linked in a white link would also have access to it, which adds a further layer of protection to the individual’s data subject rights⁴⁷⁴.

Article 49(6) of the IO Regulations set forth that the European Commission will adopt a delegated regulation on the web portal to clarify: the unique interface; the languages in which the web portal will be available, and the nature of the e-mail template. The development and

⁴⁶⁸ Articles 32(5) and 33(4) of the IO Regulations. The proceeding is laid down by the European Commission through an implementing act.

⁴⁶⁹ See Council of the EU, 7751/19, Brussels, 25 April 2019, p. 144.

⁴⁷⁰ Article 41 of IO Regulations. It must be noted that the right to restrict the processing of the contested data implies that the data at stake cannot be used pending a check on the accuracy of the data according to Article 18 GDPR.

⁴⁷¹ Confront the Commission Delegated Regulation (EU) 2021/2104.

⁴⁷² Article 49(2) of the IO Regulations.

⁴⁷³ See Articles 32(4) and 33(4) of the IO Regulations.

⁴⁷⁴ From the negotiations it is understandable that white links were discussed until their end and the information provided from the establishment of a white link was not finally incorporated in Article 33 of the IO Regulations. Although the sister Regulations do not prohibit such a possibility, we may argue that this is an essential element the European Commission could not be treated in a separated delegated act.

technical management of the web portal are delegated to eu-LISA that should make it public under the ‘.europa.eu’ URL⁴⁷⁵. eu-LISA will have the right to access and modify the web portal administration interface, without being authorised to access the data related to third country nationals⁴⁷⁶, and must ensure the confidentiality, integrity, and availability of the services and the non-repudiation of transactions⁴⁷⁷. The web portal will work by inserting in its search page the reference number of the authority competent for the manual verification procedure that is stored in the identity confirmation file of the MID⁴⁷⁸. As a result of this, the individual will be able to retrieve the data – name, postal address, e-mail address – of the authority of the Member State responsible for the manual verification of the multiple identities⁴⁷⁹. By clicking on the e-mail address, a specific request for an information template e-mail through a web form⁴⁸⁰ will be opened to facilitate further contact with the competent authority of the Member State responsible for the manual verification of the multiple identities. The template includes a field where the data subject can insert the ‘single identification number’, enabling the retrieval of the data linked in the underlying IT systems⁴⁸¹ by the competent authority of the Member State responsible for the manual verification procedure. Therefore, the reference of the authority responsible for the manual verification procedure, as well as the single identification number, must be included in the standard form so that the data subject can fill in the web portal fields⁴⁸². The template e-mail will contain a standardised request for further information. It will be available in the Member States’ official languages plus Russian, Arabic, Japanese, Chinese, Albanian, Bosnian, Macedonian, Hindi, and Turkish. The user will choose from among the language options, two of which are chosen by each Member State⁴⁸³. Once the web form is sent, ‘an automated acknowledgement e-mail shall be sent to the user, containing the contact details

⁴⁷⁵ See Article 1(1) of the Commission Delegated Regulation (EU) 2021/2104.

⁴⁷⁶ Article 4(2) of the Commission Delegated Regulation (EU) 2021/2104.

⁴⁷⁷ Article 5 of the Commission Delegated Regulation (EU) 2021/2104.

⁴⁷⁸ Article 34, letter (d), of the IO Regulations.

⁴⁷⁹ The contact details are provided by the Member States and Schengen Associated Countries and periodically reviewed by eu-LISA through pre-established single point of contact – see Article 1(3) to (5) of the Commission Delegated Regulation (EU) 2021/2104.

⁴⁸⁰ See the example provided in the Commission Delegated Regulation (EU) 2021/2104.

⁴⁸¹ Article 34, letter (c), of the IO Regulations.

⁴⁸² Article 49(4) of the IO Regulations establishes that the authorities in charge of examining and answering to these requests must be communicated to eu-LISA, that must periodically revise its actualization. The EDPS recommended realising such a revision more than once a year – see the Formal comments of the EDPS on *the draft Commission Delegated Regulations laying down detailed rules on the operation of the web portal pursuant to Regulation (EU) 2019/817 and Regulation (EU) 2019/818 of the European Parliament and of the Council*, Brussels, 31.03.2021, p. 2.

⁴⁸³ Article 3(4) of the Commission Delegated Regulation (EU) 2021/2104.

of the authority responsible to follow up this request and enabling the person to exercise the rights pursuant to Article 48(1) of Regulation (EU) 2019/817⁴⁸⁴.

From the EDPS' commentary, it is understood that the web portal will be enriched with an informative note on the protection of personal data of the individual accessible via a dedicated link on every page of the web portal, though this has not yet been published. Although welcomed, this system could have been improved so as to grant third country nationals access to clear, specific, and precise information⁴⁸⁵. The EDPS noted that the Annex II to the draft delegated act foresees, among other issues, that personal data can be transmitted to third countries and international organisations, though Article 50 of the IO Regulations prohibit, as a general rule, those operations⁴⁸⁶. Moreover, the EDPS warned that the interested person could submit complaints not only to the EDPS itself, but also to the national data protection authorities to access a judicial remedy⁴⁸⁷. Another notice will notify the individual of the rules governing the usage of the web portal that they have to accept and the consequences deriving from the submission of incorrect information⁴⁸⁸. A final disposition foreseen by the European Commission Delegated Regulation will add rules regarding the logs of the web portal⁴⁸⁹.

- Access to the web portal will be recorded, including: the Internet Protocol address of the system used by the applicant; the date and time of the request, and technical information on the environment used for the request, such as the type of device, the version of the operating system, and the model and version of the browser to enhance the quality of the service and for security purposes.
- Access to the administration interface by eu-LISA, and specifically: the identification of the user accessing the administration interface, and the actions performed on the web portal (addition, modification, or removal of content).
- Additional anonymous technical information can be collected during the usage of the web portal to optimise its usage.

This information will be kept for a maximum of two years and, the logs for accessing the web portal may be used for statistical purposes as well as to monitor the usage of the web portal

⁴⁸⁴ *Ibid.* Article 3(5).

⁴⁸⁵ Formal comments of the EDPS on *the draft Commission Delegated Regulations laying down detailed rules on the operation of the web portal pursuant to Regulation (EU) 2019/817 and Regulation (EU) 2019/818 of the European Parliament and of the Council*, Brussels, 31.03.2021.

⁴⁸⁶ See Chapter VI. Some preliminary considerations on the scope of interoperability in the external dimension of EU policies can be found at: Francesca Tassinari, "The externalisation of Europe's data protection law in Morocco: an imperative means for the management of migration flows", *Peace & Security - Paix et Sécurité Internationales (Euro Mediterranean Journal of International Law and International Relations)*, No. 9, 2021, pp. 1-24.

⁴⁸⁷ Article 46 CFREU.

⁴⁸⁸ Article 5(2) of the Commission Delegated Regulation (EU) 2021/2104.

⁴⁸⁹ Article 7 of the Commission Delegated Regulation (EU) 2021/2104.

in order to prevent any misuse, though it is not clear whether it will be the CRRS that stores these logs as the IO Regulations did not address the issue.

All in all, the web portal is an interesting tool enabling the exercise of the data subject's rights, but its usage is too constricted, as only red and white links are covered. As we noted elsewhere⁴⁹⁰, its benefits depend on the awareness data subjects will gain on their data protection rights and, consequently, on the spread of an inclusive European digital culture among existing national supervisory authorities.

ii) The individual's right to access, rectify, and erase the links

The IO Regulations set forth general norms regarding the exercise of the rights to access, rectify, and erase personal data stored in the MID – i.e., the links – by directly addressing the competent authority, as well as to exercise the right to restrict the data's processing⁴⁹¹. According to the Regulations, the individual can address any Member State that will then examine their request and answer – including through a central office – their request according to the GDPR, the LED, and the EUDPR. The request will be examined and replied to 'without undue delay' and, in any case, forty-five days within receipt of the request, this period may be extended by a further fifteen days⁴⁹².

If a request for rectification and erasure of personal data⁴⁹³ is addressed to an authority that was not the one responsible for the manual verification of different identities, then, the Member State must contact the authorities of the Member State responsible for the manual verification, or the ETIAS Central Unit, within seven days of receiving the request. When consulted, the authority responsible for the manual verification must check 'the accuracy of the data and the lawfulness of the data processing' without undue delay and in any event within thirty days of such contact – this is extendable by fifteen days depending on the complexity and number of requests at the time the contact is established⁴⁹⁴. However, neither the consulted Member State nor the ETIAS Central Unit will directly contact the interested person, instead, they must be informed by the Member State that was first contacted according to the previous procedure. It is then important to assess the issues stemming from the presence of different jurisdictions

⁴⁹⁰ Francesca Tassinari, "La transizione digitale dell'UE nello spazio di libertà, sicurezza e giustizia: le sfide dell'interoperabilità dei sistemi IT su larga scala", *Idee d'Europa*, Ferrara, 14.06.2021, available at www.futureu.europa.eu.

⁴⁹¹ Article 48 of the IO Regulations.

⁴⁹² Article 48(2) of the IO Regulations.

⁴⁹³ Requests for access and for restriction of processing are therefore excluded, which creates a significant legislative gap for the harmonised exercise of these rights.

⁴⁹⁴ Article 48(3) of the IO Regulations.

within the EU, given that it is impossible for a judge to assess the decision taken by the authority of another Member State even if it is based on the intercurrent flow of information between all States of the Union⁴⁹⁵.

If the data stored in the MID is erroneous, or has been registered in an unlawful manner, the IO Regulations establish that the Member State responsible for the manual verification of multiple identities, or the Member State to which the request for rectification or suppression of the personal data was addressed – ‘where there was no Member State responsible for the manual verification of different identities or where the ETIAS Central Unit was responsible for the manual verification of different identities’ – must rectify or suppress the data without undue delay⁴⁹⁶. Therefore, Article 48(5) of the IO Regulations leads us to understand that if the link was generated in an automated manner – that is, in cases of there being ‘no Member State responsible for the manual verification of different identities’ – the Member State to which the request was addressed is the one responsible for rectifying or suppressing the erroneous or unlawfully registered links. Although guaranteeing the individuals’ right to the protection of personal data, this solution may over-burden the authority that assumes the responsibility for any error generated by the machine. It is hard to justify the fact that the ETIAS Central Unit is not responsible for rectifying or suppressing the erroneous or unlawfully registered links it has established, but rather that this duty is delegated to the national authority that the individual has addressed. Even if this discharge of responsibility may be positive in terms of facilitating the individual’s access to a remedy, it should have been justified by the co-legislators. Indeed, the addressed authority determines the competent jurisdiction to ask for compensation if the person in question was prejudiced, by a material damage or not, because of the unlawful processing or of processing contrary to the IO Regulations⁴⁹⁷. Only if the Member State shows that it is not responsible for the damage caused, may it be exempted from liability, either totally or partially. Consequently, if the ETIAS Central Unit is responsible for an incorrect or unlawful link, the Member State to which the request for compensation is addressed should be granted the possibility to ask the EBCG Agency for compensation as the processing activities stem from the ETIAS Central Unit.

⁴⁹⁵ Mariolina Eliantonio, “Information Exchange in European Administrative Law: A Threat to Effective Judicial Protection?”, *Maastricht Journal of European and Comparative Law*, No. 3, 2016, pp. 531-549.

⁴⁹⁶ Article 48(5) of the IO Regulations.

⁴⁹⁷ Article 46 of the IO Regulations.

Interoperability falls under the net of the EU's integrated administrations, where the final decision is made by the sum of data stemming from different Member States – i.e., different jurisdictions⁴⁹⁸. According to Eliantonio:

‘The strict separation of jurisdiction also implies that if acts can be challenged only before the courts with jurisdiction on the authority issuing the measure, and if national courts cannot assess the legality of measures linked to those under direct challenge which do not fall within their jurisdiction, it is inevitable that some challenges need to be directed against measures which are initial or intermediate in the decision-making process, although liable to affect individuals' rights’⁴⁹⁹.

Thus, the fact that the data subject addresses the request for rectification or suppression to the competent authority responsible for the manual verification leaves the fact that the authority establishing the link might have counted on data stored in the underlying systems that were introduced by other Member States unresolved. Even though at the moment of the establishment of the link the authority responsible for the manual verification should check the accuracy and lawfulness of the linked data, its responsibility ends as far as the reliability of the link is concerned. Otherwise, the authority responsible for resolving a yellow link would find itself in a situation of endless responsibility covering the breaches that, in practice, it might not even be able to assess. The IO Regulations do not analyse these issues in detail and refer to the domestic law of the Member State to which the request for rectification or suppression was submitted and that should regulate the right to a remedy against the damage suffered. Consequently, potentially each one of the twenty-seven Member States' legal orders that compose the EU – plus the four belonging to the Schengen Associated Countries – will impose its own norms to guarantee the fundamental right to an effective remedy⁵⁰⁰. In case of infringement of personal data rules, including its exchange, the IO Regulations establish that the Member States must adopt ‘effective, proportionate, and dissuasive’ measures⁵⁰¹. In the specific case of the EBCG Agency, given the lack of a sanctioning power exercisable by the Executive Director of the Agency itself, Article 69 of the EUDPR applies:

‘Where an official or other servant of the Union fails to comply with the obligations laid down in this Regulation, whether intentionally or through negligence on his or her part, the official or other servant concerned shall be liable to disciplinary or other action, in accordance with the rules and procedures laid down in the Staff Regulations’.

The IO Regulations establish that the interested person is informed in writing that their data has been corrected or erased. In such cases, provided that the competent authority in charge

⁴⁹⁸ See Mariolina Eliantonio, *loc cit.*

⁴⁹⁹ *Ibid.*, p. 537.

⁵⁰⁰ Article 47 CFREU.

⁵⁰¹ Articles 83 GDPR and 57 LED.

of correcting or suppressing the links is the one updating the identity confirmation file, the MID would be re-activated and most likely generate new links. Therefore, the Member State responsible for the manual verification or the Member State to which the individual addressed its request of rectification or erasure shall establish or update the links in the identity confirmation file⁵⁰². If the data stored in the MID are considered to be correct and processed in a lawful manner, then, the authority of the Member State competent for the manual verification, or the one that receives the request from the individual, must adopt an administrative decision defining in writing the reasons underlying the why the data has not been corrected or erased. This last decision must contain the provision of the remedies available to challenge that decision *vis-à-vis* the request of access, rectification, suppression, or restriction of the processing of personal data and, ‘if it is the case’, to submit a judicial action or to present a complaint before the competent authorities, the judicial bodies, and any other body giving assistance, specifically to the national supervisory authority of the Member State in question⁵⁰³. Therefore, the individual in question may challenge the decision in the Member State of the authority competent for the manual verification procedure or, alternatively, in the Member State where they submitted the request, depending on the circumstances analysed above.

In terms of the manual verification procedure of multiple identities, it is clear which authorities are responsible, as they are notified by eu-LISA⁵⁰⁴, in the other cases, the co-legislators do not specify which authorities can be addressed. Here is clarification by way of an example: If by requesting a visa the MID establishes in an automated manner a white link with a SIS refusal of entry alert, the third country national should be denied entry to the Schengen area as a result of the alert being issued. Provided that the link was generated in an automated manner, there is no authority responsible for the manual verification procedure, but from the considerations made *supra*, the individual must be informed of the establishment of the link by the competent consular authority. This involves informing the interested person that they can exercise the right to access, rectify and suppress his/her personal data, as well as the right to restrict the data processing activity. Yet, which authority should be addressed? The Data Protection Officer? The national supervisory authority? Both? Although the co-legislators left a margin of discretion for the Member States, this confusion hampers a coordinated execution of the IO Regulations and, given that these issues are of paramount importance to safeguard

⁵⁰² Article 34 of the IO Regulations.

⁵⁰³ Article 4, point 21, GDPR.

⁵⁰⁴ Article 71(1) of Regulation (EU) 2019/817 and Article 67 of Regulation (EU) 2019/818.

Articles 8 and 47 of the CFREU, a more detailed bottom-down regulation would have been desirable.

Last but not least, Article 48(11) of the IO Regulations adds a clause on the safeguards regarding the restrictions to the right to access, rectify, suppress personal data, and to restrict the data processing activity: ‘This Article is without prejudice to any limitations and restrictions to the rights set out in this Article pursuant to Regulation (EU) 2016/679 and Directive (EU) 2016/680’. This clause recalls the GDPR and the LED⁵⁰⁵ norms on the derogations to the subjective data protection rights of individuals to access, rectify, suppress personal data as well as the restriction of the data processing activity, for example, for reasons of national security, public order, or public security. Despite this, we should recall that those limitations must be: set forth by law; respect the essence of the fundamental rights and freedoms of individuals, and necessary and proportionate in a democratic society⁵⁰⁶. Therefore, any restriction that concerns the procedure of detecting multiple identities must be established by law and, in no case can the protection granted by the Charter be lessened.

By way of conclusion, the IO Regulations establish that the Member State responsible for the manual verification of the different identities or, if applicable, the Member State to which the request has been made, shall keep a written record that a request of accession, rectification, erasure or the restriction of processing of personal data was made, clarifying elucidating how it was addressed, and the record will be made available to supervisory authorities without delay. In sum, the liability of the data protection controllers and processors must be assessed as far as Article 21 data processing activities are concerned so as to see in which ways they respond to the individual and EU institutions.

2.3.3. Querying the Common Identity Repository for the purposes of preventing, detecting, or investigating terrorist offences or other serious criminal offences: The purpose of Article 22

Those IT systems for which law enforcement authorities and Europol’s access is an ‘ancillary’ purpose⁵⁰⁷ subject the consultation for the purposes of preventing, detecting, or investigating terrorist offences or other serious criminal offences⁵⁰⁸ to strict conditions: first, a

⁵⁰⁵ Articles 25 GDPR and 15 LED.

⁵⁰⁶ Article 52(1) CFREU.

⁵⁰⁷ See Chapter IV.

⁵⁰⁸ Serious criminal offences encompass the offences of which the EU itself becomes a victim (and thus all its citizens are equally victimised by) as well as offences for which the EU has a moral obligation to intervene because it in some way facilitates the commission of transnational crimes – i.e., when the freedoms granted by the EU are abused for illegitimate purposes. See the study of the European Parliament, *Developing a Criminal Justice Area in the European Union*, PE 493.043, Brussels, 2014, p. 7, available at www.europarl.europa.eu.

cascade approach ensuring that there has been a previous check of other national databases⁵⁰⁹; second, an *ex post* authorisation if the access is granted due to urgent procedures for imminent threats to security, serious crimes, or terrorism⁵¹⁰. According to the FRA, the cascade approach lays down the principles of proportionality and of purpose limitation in the following terms:

‘[...] Give that their data are collected for a different purpose and without any connection to a criminal activity or another security risk, safeguards accompanying the access of law enforcement to this data should be particularly robust, even more so than in case of other groups of persons’⁵¹¹.

Thus, the authority should be able to state whether the individual is linked to a criminal investigation or not⁵¹². However, during the negotiations around the latest generation of large-scale IT systems promoted with the smart border package of 2016⁵¹³, it was noticeable that Member States began to see the cascade approach as an obstacle in the fight against criminal activities and started to call for its suppression⁵¹⁴.

Article 22 of the IO Regulations was presented with the purpose of suppressing these filters by allowing the query of the CIR as far as the EES, the VIS, the ETIAS, and the Eurodac are concerned⁵¹⁵ ‘when there are reasonable grounds to believe the data of an individual may be in

⁵⁰⁹ The so-called cascade approach requires to check other national databases – e.g., the system Prüm – through the crime databases of other Member States before consulting the large-scale IT systems – i.e., Article 20(1) of the 2013 Eurodac recast Regulation and Article 32(2) of the EES Regulation for Member States’ designated authorities. In the case of Europol, instead, see Article 21 of the 2013 Eurodac recast Regulation and Article 33 of the EES Regulation. To be noted that a Europol’s request to consult the EES shall be accompanied by a parallel search in the VIS.

⁵¹⁰ Article 19(3) of the 2013 Eurodac recast Regulation; Article 4(2) of the revised VIS LEA Decision; Article 31(2) of the EES Regulation, and Article 51(4) of the ETIAS Regulation.

⁵¹¹ FRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Vienna, 2018, p. 67.

⁵¹² See the Commission Staff Working Document Impact Assessment, SWD(2017) 0473 final, Strasbourg, 12.12.2017: ‘For each individual system in the ‘cascade’, authorities must first submit a reasoned request to a different authority justifying the necessity of access. This creates a considerable amount of administrative burden, results in delays, and increases the data flow potentially leading to data security risks’.

⁵¹³ See Chapter IV.

⁵¹⁴ No cascade approach is established, for example, in the case of the ETIAS – confront Article 51 and 52 of the ETIAS Regulation.

⁵¹⁵ Note that SIS and ECRIS-TCN are excluded.

the EES, the ETIAS, the VIS or Eurodac and this person is a suspect, perpetrator, or a victim of a terrorism offence or a serious crime offence’.

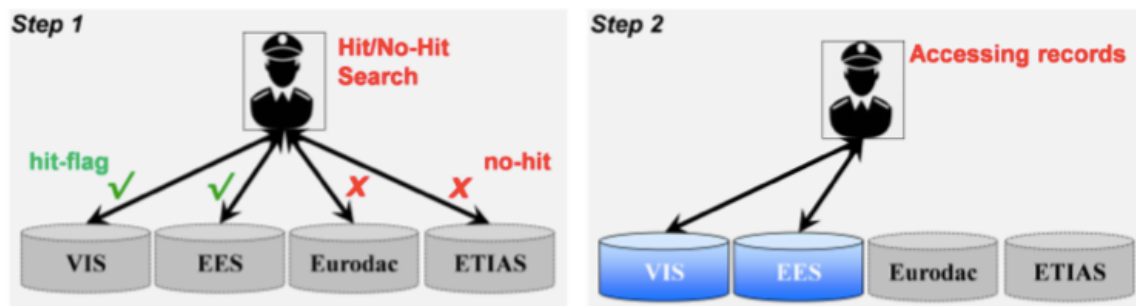


Figure 12 Two-step approach based on ‘hit-flag’ functionality – Source: Commission Staff Working Document impact assessment, SWD(2017) 473 final, Strasbourg, 12.12.2017.

The consultation of these four ‘migration systems’ through Article 22 should occur in a two-step approach that should ‘simplify’ the access of law enforcement authorities and Europol to the data stored therein so that the authorities concerned are exactly the same as those that are granted full access to the EES, the ETIAS, the VIS or the Eurodac to issues of serious crime and terrorism.

Under the first step, the authority or Europol official would input the data usually used to access the underlying system to retrieve a reference to the system containing the data matched – the so-called hit/no-hit notification – as referred to in Article 18(2) of the IO Regulations⁵¹⁶. Therefore, only the system storing the information would be visible, but not the data searched – which is not the case in ‘urgent cases’ that are foreseen in the relevant regulations. This phase is known as a ‘hit-flag’.

As part of the second step, the authority or Europol official would be granted full access to the system/s. Full access to the system/s is considered an obligation to avoid fishing expeditions⁵¹⁷. This does not mean that the authority has to access all the systems queried, since it may be sufficient to access one⁵¹⁸, but it must access it. The authority or Europol official must record their justification for not having requested full access to the data if they choose not to⁵¹⁹. We believe that this obligation impedes the objective of leaving large-scale IT systems prey to ‘fishing expeditions’⁵²⁰, though it is not clear if in case of non-compliance the national authority or the Europol staff would be sanctioned and under what terms.

⁵¹⁶ Article 22(2) of the IO Regulations.

⁵¹⁷ Article 22(2), second paragraph, of the IO Regulations.

⁵¹⁸ Article 22(1), third paragraph, of the IO Regulations.

⁵¹⁹ Article 22(1), fourth paragraph, of the IO Regulations.

⁵²⁰ Niovi Vavoula’s lecture, “EU Centralised Information Systems for Third-Country Nationals”, XX edition of the Odysseus Summer School, Brussels, from the 24 to the 4 September 2020.

In technical terms, eu-LISA was called on to develop a ‘technical solution’ enabling law enforcement authorities and Europol staff to access the CIR⁵²¹. eu-LISA proposed to reuse the architecture of the CRRS to facilitate the use of Article 78(7) and (9) of Regulation 2019/817 and of Article 74(7) and (9) of Regulation (EU) 2019/818⁵²². Even though the European Commission decision on the technical solution has not been published yet, the EDPS⁵²³ has evaluated that that Implementing Decision should have contained rules on security incidents and recommended that the categories of data to be provided by the Member States for creating reports as part of the CRRS be specified.

Article 22 has been criticised in light of the securitisation phenomenon of migration flows and the consequent stigmatisation of third country nationals⁵²⁴. In Prof. Vavoula’s belief, in the near future the use of the systems by police forces might end up assuming a central function over the other systems’ purposes⁵²⁵. Prof. Vavoula also alleges that although the current procedure is administratively cumbersome, the insertion of Article 22 has not been supported by any evidence that access was denied in the verification procedure, or that the “no answer” was given in a timely manner⁵²⁶.

Yet, on closer inspection, we believe that the so-called cascade approach was not eliminated as proposed by the European Commission thanks to the European Parliament’s firm position in safeguarding it⁵²⁷. Article 22(3) of the IO Regulations recalls that:

‘Full access to the data contained in the EES, VIS or ETIAS for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences remains subject to the conditions and procedures laid down in the respective legal instruments governing such access’.

⁵²¹ Article 74(10) of the IO Regulations provides for the establishment of ‘a technical solution’ through a European Commission’s implementing act in order to enable the Member States to: first, manage user access requests referred to in Article 22 of the IO Regulations and, second, facilitate the collection of the information to be provided to eu-LISA and the European Commission for the purpose of generating reports and statistics analysed *supra*.

⁵²² Formal comments of the EDPS on the draft Commission Implementing Decision laying down the specifications for technical solutions to manage user access requests for the purposes of Article 22 of Regulation (EU) 2019/817 and to facilitate the collection of the information for the purpose of generating reports, pursuant to Article 78(10) of Regulation (EU) 2019/817 of the European Parliament and of the Council, as well as on the draft Commission Implementing Decision laying down the specifications for technical solutions to manage user access requests for the purposes of Article 22 of Regulation (EU) 2019/818 and to facilitate the collection of the information for the purpose of generating reports, pursuant to Article 74(10) of Regulation (EU) 2019/818 of the European Parliament, Brussels, 27.09.2021, p. 2.

⁵²³ *Ibidem*.

⁵²⁴ See Niovi Vavoula, 2020, *op. cit.*, pp. 131-156, and Didier Bigo, Lina Ewert, and Elif Mendos Kuşkonmaz, “The interoperability controversy or how to fail successfully: lessons from Europe”, *Int. J. Migration and Border Studies*, Vol. 6, Nos. 1/2, 2020, pp. 93-114.

⁵²⁵ Niovi Vavoula’s lecture, “EU Centralised Information Systems for Third-Country Nationals”, XX edition of the Odysseus Summer School, Brussels, from the 24 to the 4 September 2020.

⁵²⁶ Niovi Vavoula, 2020, *op. cit.*, p. 150.

⁵²⁷ See the Council of the EU, 7751/19, Brussels, 25 April 2019, pp. 86-87.

Therefore, the author's criticism of the fact that Article 22 would suppress the *ex-post* verification on the conditions of access in urgent cases can be revisited as follows. The cascade approach, of course, does not apply in cases of 'urgency', as in these cases verification always occurs *ex post* according to the underlying legislations on large-scale IT systems. In fact, the second step foreseen by Article 22 reflects exactly the previous situation and authorisation for accessing the system is merely postponed after the first and second steps to avoid unfruitful searches. In the light of Article 22, the law enforcement authority or Europol designated authority querying the CIR will already know that the personal data they are looking for are stored in the CIR and, therefore, they will ask for access to the relevant system. A possible counterargument to our approach would show that the increasing number of reforms granting access for 'law enforcement' purposes have been promoted in the light of their incorporation to the interoperability infrastructure. However, as Prof. Vavoula highlights, such a political wave is older than the IO Regulations themselves and goes back to a historical moment when the interoperability project had been temporarily abandoned⁵²⁸.

According to the CJEU jurisprudence, terrorism and serious crimes constitute 'general interests' that legitimise the derogation of the individuals' fundamental rights to a private and family life and to the protection of personal data – see Articles 7 and 8 of the CFREU respectively regarding the limits foreseen by its own Article 52. In other words, legislative measures or activities directed at preventing, detecting, and investigating terrorist offences or other serious crimes are *prima facie* considered necessary in order to access the individuals' data stored for migration reasons. In the CJEU's words:

'[...] access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime [...]. However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities'⁵²⁹.

⁵²⁸ During the XX ed. of the Odysseus Summer School, held in Brussels between the 24 August and 4 September 2020, Prof. Vavoula's lecture on 'EU Centralised Information Systems for Third-Country Nationals' systematised the evolution of large-scale IT systems according to three historical moments: first, the 'modernisation of immigration control' stage of the 90s; second, the 'war on terror' stage developed in the 2000s and, finally, the 'quest for a security Union' characterising the years from 2010 onward. Indeed, the access of law enforcement authorities and Europol to 'migratory databases' has been promoted since the second stage with the reform of the SIS ad the Eurodac as well as the implementation of the VIS as we analysed in Chapter III.

⁵²⁹ C-203/15 and C-698/15, *Tele2 Sverige AB (C-203/15) v Post- och telestyrelsen, and Secretary of State for the Home Department (C-698/15) v Tom Watson*, para 119 – see Chapter I.

While the first sentence above authorises the access of law enforcement authorities in the context of a police investigation, the latter allows intelligence services access to the information for preventive reasons. The CJEU might have been overly imprudent to unify both topics in a single statement as this might contribute to a blurring of the lines between police and intelligence officers' functions. However, the CJEU has also advanced different conditions to lawfully restrict the individuals' fundamental rights, so that the intelligence activity must be: exceptional; directed at protecting defence or public security interests, and useful to combating such activities. In these terms, Article 22 is in line with the CJEU's position by enabling Member States and Europol's designated authorities to consult the CIR when there are reasonable grounds to believe that the consultation of EU information systems 'will contribute to the prevention, detection or investigation of terrorist offences or other serious criminal offences, in particular where there is a suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offences'. That is to say, when they believe that one of the underlying systems stores the personal data of a specific person.

From our perspective, two further concerns arise from Article 22. First, with the first query national authorities and EU agencies already know if and where personal data is recorded in one or more of the underlying IT systems. The co-legislators left the governing of the conditions for which (subsequent) full access can be obtained to the rules laid down in the respective legal instruments⁵³⁰. However, the first query already allows users to understand if and where the data is stored, notwithstanding if full-access is granted or not. Provided that the 'hit-flag' information is related to an identified or identifiable person⁵³¹, this "preview" should be in line with the law enforcement authority's access rights – i.e., the 'hit-flag' must be visible only if they have access to the underlying system. Second, Article 22 cannot impede the co-legislators from amending the underlying legislations so as to suppress *de facto* the cascade approach, while making interoperability Article 22 the prevailing legislation. If we take the revised VIS as an example, this does not seem to be happening for the time being. Its new Article 22o(1)(d) sets forth that 'a query to the CIR according to Article 22 of Regulation 2019/817 and the reply indicating that data is stored in the VIS' is a prerequisite for the designated authorities to access the VIS for law enforcement purposes. In other words, Article 22 has been added to the existing list⁵³² of requisites to access the VIS for law enforcement purposes which we believe to be a

⁵³⁰ Article 22(3) of the IO Regulations.

⁵³¹ Opinion of the EDPS No. 4/2018 on *the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, Brussels, 18.04.2018, p. 16.

⁵³² Article 22(o)(1) of the VIS revised Regulation also requires that: the consultation is necessary and proportionate for the purposes of the prevention, detection or investigation of a terrorist offence or other serious criminal offence; the consultation is necessary and proportionate in a specific case; and reasonable grounds exist to consider that

positive, as it enhances the expectation that the system contains data of interest. However, the Proposal for a Prüm II Regulation providing for the implementation of a ‘router’ enabling the simultaneous query of the Member States’ databases, the Europol data and the CIR via the ESP⁵³³, requires the EES, VIS, and ETIAS designated authorities to comply with the following requisite alone: Article 22 would be applicable when it is likely that data of a suspect, perpetrator or victim of a terrorist offence or other serious criminal offences is stored in the CIR. Article 39 of the Proposal for a Prüm II Regulation clearly refers to Article 22 of the IO Regulations regarding the launch of simultaneous queries. The possibility that the Member States’ databases are ‘simultaneously’ queried together with the CIR – i.e., some of the systems’ personal data – and the Europol data would end up suppressing the cascade approach. In other words, it is not clear whether the existence of further requisites set forth in the underlying legislations would be respected anymore. Is this another attempt to suppress the cascade approach?

2.4. Measures supporting interoperability

Other provisions supporting interoperability relate to⁵³⁴:

- improving data quality;
- the universal message format (UMF), and
- the CRRS (Central Repository for Reporting and Statistics).

2.4.1. Improving data quality and harmonising the quality requirements for the data stored in the Union’s large-scale IT systems

Article 37 sets forth that eu-LISA shall establish automated data quality control mechanisms and procedures with regard to the data stored in the systems, the sBMS and the CIR. With the support of the CRRS⁵³⁵, eu-LISA regularly submits reports on the automated data quality control mechanisms and procedures and the common data quality indicators to the Member

consultation of VIS data will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation.

⁵³³ Article 39 of the Proposal for a Regulation of the European Parliament and of the Council, COM(2021) 784 final, Brussels, 8.12.2021.

⁵³⁴ Articles 37-39 of the IO Regulations.

⁵³⁵ Commission Implementing Regulation (EU) 2021/2225 of 16 November 2021 laying down the details of the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum quality standards for storage of data, pursuant to Article 37(4) of Regulation (EU) 2019/817 of the European Parliament and of the Council, C/2021/6719, OJ L 448, 15.12.2021, pp. 23-31.

States and the European Commission⁵³⁶ while notifying the European Parliament, the Council of the EU, the EDPS, the EDPB and the FRA of the evaluation report⁵³⁷. From these reports, eu-LISA may decide, after consulting with the Advisory Groups for each of the EU information systems and the one for interoperability, to amend the values, standards, blocking and soft rules that are found to be no longer appropriate⁵³⁸.

All data has to meet minimum quality standards before it is entered into the sBMS and the CIR to achieve the purposes of interoperability. Harmonised quality standards represent quite a difficult goal to meet, provided that the data has so far been processed in silos and each IT system applies its own data quality rules⁵³⁹. This implies that divergent solutions have been found for the quality of the data and that each IT system is equipped with its own types of hardware and software.

Highly variable levels of quality among the different biometric samples may undermine the reliability of the results stemming from the interoperability components, first of all of the sBMS⁵⁴⁰. Therefore, minimum quality standards become indispensable for the functioning of the entire interoperability architecture. According to the Croatian Presidency:

‘[...] a critical success factor for the successful implementation of interoperability is the ability to collect data and share information in a structured and harmonised way. The development, endorsement and implementation of common standards in several areas is key’⁵⁴¹.

Within the Council’s Working Party on JHA Information Exchange (IXIM), five main working areas were highlighted:

- the quality of biometric data;
- the devices for the acquisition of raw biometric data;
- the quality of alphanumeric data;
- the mobile devices and solutions for access to information available through the new interoperability architecture, and
- cybersecurity⁵⁴².

⁵³⁶ Article 37(3) of the IO Regulations.

⁵³⁷ Article 37(5), second paragraph, of the IO Regulations.

⁵³⁸ Article 5(4)(c) to (e) of the Commission Implementing Regulation (EU) 2021/2225.

⁵³⁹ eu-LISA, *Shared Biometric Matching Service (sBMS), Feasibility Study - final report*, Tallin, 2018, contemplating as a second option the non-alignment of thresholds for which the sBMS would have only supported the systems by establishing according to their diverse nature. From a technical perspective, this solution might have reduced the performance of the interoperability infrastructure, for example, for searching samples complying with another system’s requirements.

⁵⁴⁰ On the sBMS performance see above.

⁵⁴¹ Council of the EU, *Horizontal overview of the biometric data quality and format standards to ensure compatibility of different IT systems in the context of interoperability*, 5924/20, Brussels, 20 February 2020, p. 2.

⁵⁴² Council of the EU, *Structure and main principles of the roadmap for standardisation for data quality purposes - Presidency discussion paper*, 7125/20, Brussels, 15 April 2020, p. 3.

First of all, data quality impacts the outcome of biometric recognition processing as inaccuracy may prevent the data from matching⁵⁴³ or lead to an erroneous result⁵⁴⁴, which would alter the entire recognition procedure. High biometric data quality avoids, for example, false-positive matches against SIS-entries as well as false-negative matches against the VIS for *bona fide* travellers and, consequently, it minimises error rates. Fingerprint quality depends on a variety of elements, including: age, whether the individual does manual work, the humidity, whether the fingers were dry, wet or dirty, unintentional as well as deliberate injuries to the fingertips, a lack of training and technical difficulties. Thus, the FRA suggests taking fingerprints through paper with ink rather than with a scanning device⁵⁴⁵. Facial images are even more sensitive and suffer from: interaction with the scanning staff (physical and behavioural); the physical environment, equipment and processing systems; their outdoor operation; the photograph's background and object occlusion; temperature and humidity; illumination and light reflection; ergonomics; the time elapsed since the acquisition of the image; age; gender; ethnic origin and skin conditions. Consequently, and although feasible, the FRA warned that the extraction of biometric templates from photographs is not a reliable solution and that live taken facial images should be preferred. In general terms, we recall that the capturing and enrolment of raw biometric data is a delicate operation that requires the presence of biometric experts and special attention should be given to the circumstances surrounding their activities. For example, while the data stored in the ECRIS-TCN is expected to be highly reliable as they are stored as part of a judicial proceeding, asylum applicants' data is usually taken in precarious conditions – e.g., in the hotspots upon their arrival in the Schengen area or following a search and rescue operation according to the latest Eurodac Proposal⁵⁴⁶. According to the FRA:

⁵⁴³ We recall that the “failure of acquisition” means the inability of the system to obtain or retrieve the image for a given data due, for example, to a quality deficiency of the image or a small number of components. The “registration failure”, instead, means the inability of the system to extract sufficient elements to generate replicate templates and occurs, for example, when fingerprint fingerprints from the intended person are not obtained.

⁵⁴⁴ The main causes of error result from the poor quality of the mechanical appliances which read these data, both as regards the lack of preparation of the staff responsible for collecting them. Therefore, the phase of the first storage is crucial for the purpose of the future verifications and should be deployed with the highest degree of professionalism – see Patrick Grother, “Interoperable Performance”, in Li Stan Z., Jain Anil K., *Encyclopedia of Biometrics*, 2015, pp. 941-946, p. 942.

⁵⁴⁵ FRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Vienna, 2018, p. 90, and the National Institute of Standards and Technology (NIST), *Fingerprint Vendor Technology Evaluation*, 2015, p. 5, available at www.nvloubs.nist.gov: ‘A live-scan sensor refers to the type of sensor that digitally records the friction ridges of a finger through techniques such as electrical or optical sensing. Scanned ink is the process of creating a digital image by using an image scanner to optically capture from paper images of friction ridges created by a finger covered with ink’.

⁵⁴⁶ See Chapter IV.

‘[...] data quality standards for collecting fingerprints in Eurodac, which mainly holds personal data on asylum applicants, are higher than standards for collecting biometric data in VIS, for which a “zero-failure to enroll initiative” is applied, following requests by Member States. This means that for VIS the individual Member States are responsible for controlling the quality, whereas for Eurodac this is centrally carried out by eu-LISA’⁵⁴⁷.

We believe that the co-legislators might have foreseen the introduction of additional safeguards to protect vulnerable groups and, above all, children. Children’s biometrics are subjected to more substantial changes than those of adults and, consequently, it would have been preferred to update them more frequently than with adults⁵⁴⁸. Additionally, the quality of alphanumeric data must be assessed on the basis of the circumstances surrounding the storage of this type of data. Travel document data, for example, carries different degrees of liability if it is considered that its authenticity may be verified (e.g., by consular authorities and border guards in the cases of the EES and the VIS respectively), partially verified (e.g., for the SIS lost, false, and stolen documents) or not verified at all (e.g., in the case of asylum seekers for which it is difficult to verify the authenticity of the documents entered in the Eurodac and in the case of the ETIAS documents as these are purely declarative)⁵⁴⁹. Although the CIR itself has been equipped to detect some of these errors, e.g., transliteration or misspelling, competent authorities should be trained in order to discover, avoid or correct the existence of errors as soon as possible. Given the above, the right to access, rectify and erase personal data is of paramount importance and the individual can positively contribute to keeping the data updated.

It should be appreciated that under the Croatian Presidency discussions were advanced on investments in the testing of relevant devices and on the development of a whitelist of devices compatible with the interoperability components that Member States could use in their procurement procedures and in technical implementation⁵⁵⁰. In the case of the MID, for example, high-quality standards are needed in the testing phase to issue correct inferences and predictions within the multiple-identity detection procedure. Provided that “real data” should not be used for testing purposes or, even better, the reconstruction of the data should not be possible in this type of operations⁵⁵¹, their usage in the frame of the IO Regulations has been (questionably) justified in light of the deployment of a research activity seeking ‘accuracy

⁵⁴⁷ FRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Vienna, 2018, p. 15.

⁵⁴⁸ *Ibid.*, p. 11, and FRA, *Fundamental rights and the interoperability of EU information systems: borders and security*, Vienna, 2017, p. 36.

⁵⁴⁹ European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 29.

⁵⁵⁰ Council of the EU, 5924/20, Brussels, 20 February 2020, p. 4.

⁵⁵¹ EDPS Opinion No. 07/2016 on *the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations)*, Brussels, 21.09.2016, p. 15: ‘However, once personal data may be used for testing purposes there is no additional safeguard on who can access those data and how and when such data may be used (e.g.: what kind of safeguards should eu-LISA implement when employing external contractors for performing those tests?)’.

standards'⁵⁵². Interoperability is expected to harmonise data quality requisites through the establishment of common data quality indicators and minimum data quality standards⁵⁵³. The former includes parameters that are taken into account when it comes to assessing the quality of the data which include the following⁵⁵⁴:

- completeness, assessing the degree to which the input data has value across all the expected attributes and related requirements in a specific use case;
- accuracy, evaluating the degree to which the input data represents how close estimates might be to the unknown true values;
- uniqueness, i.e. the degree to which the input data is not duplicated in the same EU information system or interoperability component⁵⁵⁵;
- timeliness, computing the degree to which the input data is provided within a predefined data or time that conditions the validity of the data or its use case, and
- consistency, measuring the degree to which the input data has attributes that are free from contradiction and are coherent with other data in a specific use case.

In the case of biometrics, 'resolution' will be estimated based on the degree to which the input data contains the required number of points, or pixels by unit of length. Minimum data quality standards, instead, impose the creation of minimum standard thresholds applied to each indicator. This task is assigned to eu-LISA together with the European Commission and the Member States that must agree on the values for quality standards in the context of the Interoperability Advisory Group. eu-LISA is also called on to ensure that the data quality rules remain appropriate for achieving the objectives of the EU information systems and interoperability components over the course of time⁵⁵⁶.

The European Commission implementing act on automated data quality control mechanisms and procedures establishes blocking and soft rules⁵⁵⁷ to assess the degree with which any data entered in the systems and in the interoperability component – so-called 'input data' – is

⁵⁵² Article 5(1)(b) GDPR.

⁵⁵³ Article 37(2) of the IO Regulations and Article 1(1) of Commission Implementing Regulation (EU) 2021/2225.

⁵⁵⁴ See Article 6 of Commission Implementing Regulation (EU) 2021/2225.

⁵⁵⁵ See Article 3(6) of Commission Implementing Regulation (EU) 2021/2225.

⁵⁵⁶ Article 5 of Commission Implementing Regulation (EU) 2021/2225.

⁵⁵⁷ According to Article 2(d) and (e) of Commission Implementing Regulation (EU) 2021/2225 'blocking rules' are 'rules or a set of rules that measure the degree to which data are compliant to defined data requirements conditioning their storage and or use'; 'soft rules' are 'rules or a set of rules that measure the degree to which the input data is compliant with the defined data requirements conditioning its relevance and/or optimal use'. While the former issue an alerts to the user that impedes the entrance and storage of the data for non-compliance, the latter enables the entrance and storage of the data though a quality issue flag, notification, or warning message is added.

compliant with the data requirements⁵⁵⁸. In practice, data that does not comply with the interoperability quality standards laid down by the European Commission in its Implementing Regulation on data quality control mechanisms and procedures, the common data quality indicators and the minimum quality standards⁵⁵⁹ cannot be hosted – i.e., is rejected – by the interoperability infrastructure, which safeguards the performance of its mechanisms⁵⁶⁰. Conversely, data with good, or low-quality standards can be entered into the systems and interoperability components, though the latter is labelled with ‘a data quality alert’ that calls for rectification.

The establishment of minimum data quality standards is quite a delicate issue: on the one hand, high minimum standards provoke the rejection of raw data that might constitute precious and unique information, for example, if the data was collected at a crime scene as happens with SIS latent data; on the other hand, lower quality standards would feed the interoperability components with bad information that undermines its reliability. For the purpose of maintaining high-quality data, the IO Regulations introduce an ‘issue detection mechanism’ and a ‘data cleaning mechanism’⁵⁶¹ for the data stored in the SIS and the CIR, which are new additions to the framework of the legislation regulating the IT systems. The issue detection mechanism aims at carrying out checks to identify data that no longer meets the data quality rules or standards related to data quality indicators. Yet, this mechanism cannot lead to the deletion of the affected data. Such a mechanism is run in an automated manner, or by eu-LISA on an *ad hoc* basis after consulting the Advisory Group of the EU information system or the interoperability Advisory Group. The data cleaning mechanism, instead, consists of an automated process to detect data for which the retention period is less than the time defined in the legislation governing the relevant EU information system or interoperability component and must inform the Member State of the scheduled erasure of the data. Two main scenarios can be depicted:

- first, the possibility that the rules on quality change in a way that is incompatible with the data already stored in the systems and the interoperability components, or
- second, that the deadline for the retention of the data has expired.

This mechanism presents the interoperability components a useful tool for combating the unlawful retention of personal data in respect of the different deadlines established by the

⁵⁵⁸ See the Formal comments of the EDPS on *the draft Commission Implementing Regulations laying down the details of the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum quality standards for storage of data pursuant to Article 37(4) of Regulation (EU) 2019/817 and Article 37(4) of Regulation (EU) 2019/818 of the European Parliament and of the Council*, Brussels, 30.04.2021.

⁵⁵⁹ Article 37(4) of the IO Regulations.

⁵⁶⁰ The system of blocking and soft rules described in Article 4 of the IO Regulation, indeed, will also allow to calculate the percentage of the data quality with respect to the highly parameters.

⁵⁶¹ Article 2(4) and (5) of Commission Implementing Regulation (EU) 2021/2225.

underlying IT systems and the interoperability components⁵⁶². However, the complexity and uniqueness of such a mechanism calls on for the training of national authorities in order that they learn how to properly manage the components⁵⁶³ – especially as far as the MID manual verification procedure is concerned.

2.4.2. The Universal Message Format (UMF)

Communication among users, central systems, and the CIR is facilitated by a UMF enabling the exchange of cross-border information between IT systems, authorities, or organisations in the JHA fields⁵⁶⁴. The UMF proposed by the IO Regulations is built upon a wider project on UMF governance that aims at facilitating the exchange of information among the Member States' law enforcement agencies⁵⁶⁵. The project is coordinated by the German Bundeskriminalamt⁵⁶⁶.

The UMF will provide large-scale IT systems with a unique language while avoiding adapting the ESP and the CIR to each system's ICD⁵⁶⁷. In practice, the UMF is expected to lay down a common vocabulary and logical structure to exchange the information, notwithstanding the underlying legal framework – e.g., the Swedish Initiative, the Prüm hit procedure, the access

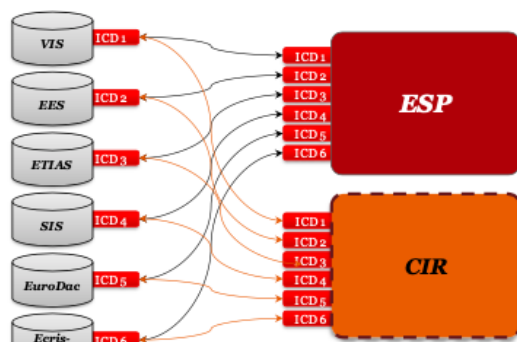


Figure 13 Messages exchange without UMF – Source: Feasibility study on a Common Identity Repository (CIR).

to Europol data, and so on. As the German Delegation pointed out:

‘Ideally, UMF3 should be a European exchange standard for law enforcement authorities (LEAs) which is used in case of system adaptations or the development of new systems. The use of the

⁵⁶² The data are to be destroyed irreversibly at the end of the data retention period, see C-203/15 and C-698/15, *Tele2 Sverige AB (C-203/15) v Post- och telestyrelsen and Secretary of State for the Home Department (C-698/15) v Tom Watson, Peter Brice, Geoffrey Lewis*, para. 122, and C-293/12 and C-594/12, *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources*, paras. 66 to 68.

⁵⁶³ See Article 2(2)(g) among the interoperability objectives for which ‘facilitating and supporting technical and operational implementation by Member States of EU information systems’. Trainings are mainly assigned to eu-LISA but there might be other channels like CEPOL, and also the own Member States are responsible for preparing their own authorities.

⁵⁶⁴ Article 38 of the IO Regulations.

⁵⁶⁵ See the Note from the German Delegation in Council of the EU, *Universal Message Format (UMF) 3 Proposal for the 5th IMS action list*, 6882/16, Brussels, 10 March 2016, and the “New documents reveal Europol’s plans to increase surveillance”, *EDRI*, 24 August, 2016, available at www.edri.org.

⁵⁶⁶ See the Note from the German Delegation in Council of the EU, *Universal Message Format (UMF) 3 Proposal for the 5th IMS action list*, 6882/16, Brussels, 10 March 2016.

⁵⁶⁷ Article 38 of the IO Regulations. An overview on the message formats with or without a UMF is available in the European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017, p. 66.

standard is a gradual process which is going to take many years. Therefore, we need to develop an organizational form, the governance model, in order to guarantee the maintenance and further development of the standard⁵⁶⁸.

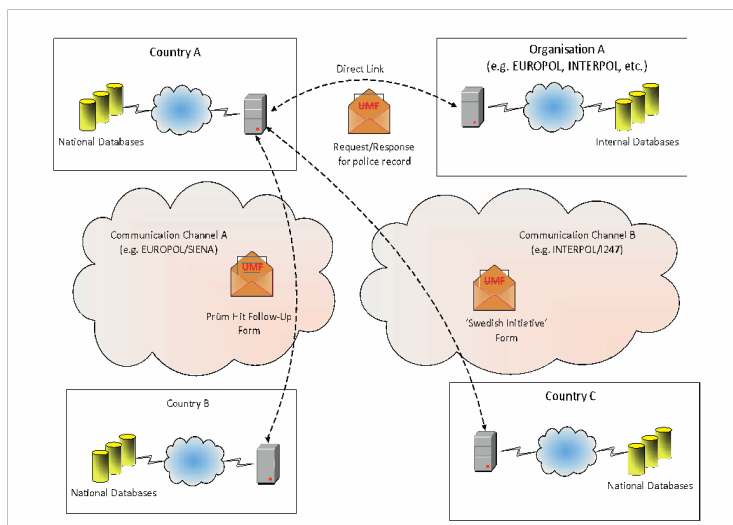


Figure 14 UMF as a layer between systems – Source: Universal Message Format. Faster, cheaper, better, Brussels, 24-04.2014.

Six pilot projects were launched in 2016 by Europol and five Member States: Estonia, Finland, Greece, Poland, and Spain. In the case of Europol, specifically, the QUEST is a web application that allows the Member States to search inside the information in the Europol Information System (EIS)⁵⁶⁹. Member States, on their part, developed a software to simultaneously query their national

databases and the EIS.

The UMF3 will be applied to EES, ETIAS, Eurodac, ECRIS-TCN, ESP, CIR, MID, and other forthcoming information systems developed in the JHA area⁵⁷⁰. In these terms, the interoperability UMF is deemed to be a model for any cross-border information exchange among law enforcement bodies ‘to orchestrate interactions between multiple systems in an interoperable way’⁵⁷¹. The standards applied by the IO Regulations will be laid down by the European Commission in an implementing act adopted following the examination procedure⁵⁷².

2.4.3. The Central Repository for Reports and Statistics (CRRS)

eu-LISA is delegated the task of anonymising⁵⁷³ the data extracted from the relevant IT systems and the interoperability components with an automated mechanism⁵⁷⁴ through which

⁵⁶⁸ See the Note from the German Delegation in Council of the EU, *Universal Message Format (UMF) 3 Proposal for the 5th IMS action list*, 6882/16, Brussels, 10 March 2016, p. 2.

⁵⁶⁹ See Chapter VI.

⁵⁷⁰ Article 38(2) of the IO Regulations.

⁵⁷¹ See the High-level expert group on information systems and interoperability, *Final report*, Ares(2017)2412067, Brussels, 11.05.2017.

⁵⁷² Article 38 of the IO Regulations.

⁵⁷³ We should recall that in C-524/06, *Heinz Huber v Bundesrepublik Deutschland*, paras. 63-68, the CJEU sentenced that the storage of personal data containing individualised information in the German Central Register of Foreign Nationals for statistical purposes, was not necessary in the light of Article 7(e) of the DPD.

⁵⁷⁴ For which purpose eu-LISA shall be considered as the processor of the CRRS data according to Article 7 of the Commission Delegated Regulation (EU) 2021/2223 of 30 September 2021 supplementing Regulation (EU)

irreversible identification is achieved⁵⁷⁵. Among this data, ‘critical identity data’⁵⁷⁶ will be processed, that is: name; first name; surname; family name; given names; the alias of any person whose data might be stored in any EU information system; the number of travel documents; address (street name, house number) of the individual; their telephone number, and Internet Protocol address. ‘Critical identity data’ does not always fall within the definition of ‘identity data’ according to the IO Regulations, but does contain data that might lead to the disclosure of the identity of the person unless anonymised. Anonymised data will be held in the CRRS. Technically speaking, the CRRS is made of:

- the tools necessary for anonymising data;
- a central infrastructure, consisting of a repository of anonymous data, and
- a secure communication infrastructure to connect the CRRS to the EES, VIS, ETIAS, SIS, Eurodac and ECRIS-TCN, as well as the central infrastructures of the sBMS, the CIR and the MID.

First of all, the CRRS will produce and store data, statistics, and technical reports⁵⁷⁷ regarding the functioning of the interoperability components⁵⁷⁸. Reports and statistics concerning the interoperability components relate to⁵⁷⁹:

- concerning the ESP, the number of queries as a whole and the number of queries to each of the Interpol databases;
- concerning the CIR:
 - the number of queries for the purposes of Articles 20, 21 and 22 of the IO Regulations;
 - nationality, gender and year of birth of the person being searched for;

2019/817 of the European Parliament and of the Council with detailed rules on the operation of the central repository for reporting and statistics, C/2021/4982, OJL 448, 15.12.2021, pp. 7-13.

⁵⁷⁵ Further processing of personal anonymised data – which is not a synonym of pseudonymisations that prevents the identification of the data subject without the use of additional information and it is generally done by assigning a code and the physical separation of these set of data by virtue of Article 4(5) GDPR – is always compatible with the purpose limitation principle – see Article 39 and 66 of the IO Regulations.

⁵⁷⁶ Article 1(4) of the Commission Delegated Regulation (EU) 2021/2223.

⁵⁷⁷ Article 1(2) of the Commission Delegated Regulation (EU) 2021/2223 establishes that (statistical) reports’ means ‘an organised collection of statistical data, produced by the central repository in an automated manner according to a set of pre-established rules and stored in the central repository’.

⁵⁷⁸ Article 66 of Regulation (EU) 2019/817 and Article 62 of Regulation (EU) 2019/818 respectively. Article 78(1) of Regulation (EU) 2019/817 also foresees the eu-LISA should monitor the development of the interoperability components and their connection to the national uniform interface for technical output, cost-effectiveness, security and quality of service.

⁵⁷⁹ Article 66 of Regulation (EU) 2019/817 and Article 62 of Regulation (EU) 2019/818. In case the Proposal for a Regulation of the European Parliament and of the Council, COM(2021) 784 final, Brussels, 8.12.2021, will be adopted, then the CRRS is expected to store reports and statistics for the Prüm II purposes according to its Article 71.

- the type of the travel document and the three-letter code of the issuing country, and
- the number of searches conducted with and without biometric data;
- concerning the MID:
 - the number of searches conducted with and without biometric data;
 - the number of each type of link and the EU information systems containing the linked data, and
 - the period of time for which a yellow and red link remained in the system.

Reports and statistics on the interoperability components are needed for auditing purposes. Four years after the start of operations of each interoperability component in accordance with Article 72 of Regulation (EU) 2019/817 and Article 68 of Regulation (EU) 2019/818⁵⁸⁰ – and every four years thereafter – eu-LISA shall submit to the European Parliament, the Council and the Commission a report on the technical functioning of the interoperability components, including their security. As for the European Commission, one year after each report issued by eu-LISA and with the support of the latter⁵⁸¹, it shall produce an overall evaluation of the interoperability components for the European Parliament, the Council, the EDPS and the FRA. Among other topics, the overall evaluation must examine the results achieved against the objectives of the IO Regulations and their impact on fundamental rights, including, in particular, an assessment of the impact of the interoperability components on the right to non-discrimination⁵⁸². In this regard, a specific provision has been inserted regarding the MID, for which two years after the start of operations and in accordance with 72(4) of Regulation (EU) 2019/817 and Article 68(4) of Regulation (EU) 2019/818, the European Commission shall produce an examination of the impact of the MID on the right to non-discrimination⁵⁸³. The Member States and Europol shall provide eu-LISA and the European Commission with the information necessary to draft the above-mentioned reports ‘without jeopardising working

⁵⁸⁰ See *supra*.

⁵⁸¹ Article 78(8) of Regulation (EU) 2019/817 and Article 74(8) of Regulation (EU) 2019/818.

⁵⁸² The overall evaluation shall include any necessary recommendations, concerning: an assessment of the application of the IO Regulations; an assessment of the functioning of the web portal, including figures regarding the use of the web portal and the number of requests that were resolved; an assessment of the continuing validity of the underlying rationale of the interoperability components; an assessment of the security of the interoperability components; an assessment of the use of the CIR for identification; an assessment of the use of the CIR for preventing, detecting or investigating terrorist offences or other serious criminal offences; an assessment of any implications, including any disproportionate impact on the flow of traffic at border crossing points and those with a budgetary impact on the general budget of the Union; an assessment of the search of the Interpol databases via the ESP, including information on the number of matches against Interpol databases and information on any problems encountered.

⁵⁸³ Article 78(6) of Regulation (EU) 2019/817 and Article 74(6) of Regulation (EU) 2019/818.

methods or include information that reveals sources, staff members or investigations of the designated authorities'⁵⁸⁴.

Moreover, the CRRS is attributed a supporting function as far as the other IT systems' objectives are concerned. For this purpose, the CRRS will enable the elaboration of business reports, that is, 'cross-system statistical data and analytical reporting for policy, operational and data quality purposes'⁵⁸⁵. The CRRS will merge the single repositories of data and statistics laid down in the regulations underpinning each large-scale IT system⁵⁸⁶ the data from which will be pushed by the large-scale IT systems to the CRRS⁵⁸⁷, logically separated by the EU information system and anonymised. Article 39(2) of the IO Regulations states that business reports and technical reports will be provided according to:

- Article 63 of the EES Regulation;
- Article 17 of the VIS revised Regulation;
- Article 84 of the ETIAS Regulation;
- Article 60 of the SIS Regulation (EU) 2018/1861;
- Article 16 of the SIS Regulation (EU) 2018/1860;
- Article 74 of the SIS Regulation (EU) 2018/1862, and
- Article 32 of the ECRIS-TCN Regulation.

The technical reports shall contain 'statistics on the usage of the system, availability, incidents, performance capacity, biometric accuracy, data quality, and, where applicable, pending transactions'⁵⁸⁸. The business reports produced by the CRRS, instead, shall be 'customisable by the user in order to allow the filtering or grouping of the data by means of a reporting tool made available together with the CRRS'⁵⁸⁹. In other words, Member States could ask eu-LISA to create customisable reports and statistics – that is, reports and statistics based on specific, contextual, and even *ad hoc* needs – for border checks, visa, migration and security policy-making in the Union:

'Upon request, relevant information shall be made available by the Commission to the European Union Agency for Fundamental Rights in order to evaluate the impact of this Regulation on fundamental rights'⁵⁹⁰.

Business reports are the greatest advance stemming from the CRRS to further the realisation of cross-system statistical data according to the provisions (and limits) set forth in the legislation

⁵⁸⁴ Article 78(7) of Regulation (EU) 2019/817 and Article 74(7) of Regulation (EU) 2019/818.

⁵⁸⁵ Article 39(2) of the IO Regulations.

⁵⁸⁶ Article 39(2) of the IO Regulations.

⁵⁸⁷ eu-LISA, *Elaboration of a Future Architecture for Interoperable IT Systems at eu-LISA*, Tallin, 2019, p. 11.

⁵⁸⁸ Article 2(6) of the Commission Delegated Regulation (EU) 2021/2223.

⁵⁸⁹ Article 2(7) of the Commission Delegated Regulation (EU) 2021/2223.

⁵⁹⁰ Article 66(7) of Regulation (EU) 2019/817 and 62(7) of Regulation (EU) 2019/818.

pertaining to each system⁵⁹¹. The CRRS will complement the ETIAS Regulation that allows the creation of EES-ETIAS cross-system statistics for the specific purpose of developing the so-called screening rules⁵⁹². Cross-system statistics will enable the discovery of various trends, e.g.: the percentage of visa overstayers by country of first entry, grouped by third country, and the percentages of nationalities that enter a Member State different than the one indicated on the visa application – i.e., by combining EES and VIS’ data; the distribution of fingerprint quality by Member State, or the nationalities of visa holders that are also asylum applicants – i.e., combining VIS and Eurodac data. In sum, the CRRS will become an attractive tool for orientating the co-legislators while submitting new policy proposals.

We must note that access to the CRRS is granted not only to Member States’ authorities, the European Commission, and eu-LISA ‘by means of controlled, secured access and specific user profiles, solely for the purpose of reporting and statistics’⁵⁹³, but also to the ETIAS Central Unit of the EBCG Agency and to Europol. The former could access the data concerning the ESP, the CIR, and the MID for the purpose of carrying out risk analyses within the monitoring of migratory flow, vulnerability assessments⁵⁹⁴ and the SCH-EVAL. The latter might access the CRRS with regard to data concerning the CIR and the MID for the purpose of carrying out strategic, thematic, and operational analyses⁵⁹⁵. Notably, Article 48(9) of Regulation (EU) 2019/817 and Article 74(9) of Regulation (EU) 2019/818 add that Member States and Europol ‘shall prepare annual reports on the effectiveness of access to data stored in the CIR for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences’. The reports and statistics shall be transmitted to the European Commission by 30 June of the subsequent year and should cover, for example, the reasonable grounds given for a substantiated suspicion that a suspect, perpetrator or victim is covered by the EES Regulation, the revised VIS Regulation, the ETIAS Regulation, and in the future, Eurodac, according to Article 22 of the IO Regulations. In addition, the annual report should highlight the number and

⁵⁹¹ In case new statistics, including cross-system statistics, are needed for Member States or Union agencies, the underlying legislation should be amended accordingly.

⁵⁹² See Chapter IV.

⁵⁹³ See Article 39(2) *in fine* of IO Regulations.

⁵⁹⁴ Article 66(4) of Regulation (EU) 2019/817 and 62(4) of Regulation (EU) 2019/818. To be noted that the EBCG Agency can also ask eu-LISA to prepare reports and statistics for risk analyses and vulnerability assessments in the SIS Regulation (EU) 2018/1861 and SIS Regulation (EU) 2018/1862. See, for example, the Council of the EU, *Risk Analysis for 2019*, 1218/2019, Warsaw, 2019, available at www.frontex.europa.eu.

⁵⁹⁵ Article 66(5) of Regulation (EU) 2019/817 and 62(5) of Regulation (EU) 2019/81. See Article 18(2)(b) and (c) of Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, *OJ L* 135, 24.5.2016, pp. 53-114 (Europol Regulation hereinafter).

types of cases that have ended in successful identifications⁵⁹⁶. Unfortunately, reports by Member States and Europol might not be published for reasons of security and public order, to prevent crime, and to guarantee that no national investigation is jeopardised⁵⁹⁷. As a result, it would have been beneficial to also include the European Parliament in the reporting process to enhance the democratic control over Article 22 of the IO Regulations.

⁵⁹⁶ Other fields concern: the exact purposes of the consultations including the types of terrorist offences or other serious criminal offences; the number of requests for access to the CIR for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences, and the need and use made of the exceptions for cases of urgency including those cases where that urgency was not accepted by the ex-post verification carried out by the central access point.

⁵⁹⁷ Article 78(1) of Regulation (EU) 2019/817 and Article 74(10) of Regulation 2019/818.

CHAPTER VI

GLOBAL INTEROPERABILITY IN THE EUROPEAN UNION'S AREA OF FREEDOM, SECURITY AND JUSTICE

As soon as interoperability first emerged in the freedom, security and justice discourse, Prof. De Hert envisaged that the interoperability of large-scale IT systems would go beyond the Union's borders, and he firmly maintained that such a form of cooperation should have been implemented only in exceptional circumstances based on the principle of reciprocity¹. According to Prof. De Hert and Prof. Gutwirth, '[i]n practice this means no common technical platforms, no (more) global interoperable keys, no global principle of availability, but exceptional *ad hoc* transfers of data between police forces in respect of the principles laid down in agreements on criminal cooperation and data protection regulations'². However, the latest IT advances suggest that 'global interoperability' may be a valuable solution to easily exchange information in respect of each legal order's laws. In Palfrey and Gasser's words:

'One of the tricks to the creation of interoperable systems is to determine what the optimal level of interoperability is: in what ways should the systems work together, and in what ways should they not?'³

Thus, the key issue is to assess how desirable interoperability is, or in other words, which kind of interoperability is lawful and sustainable – i.e., consistent – *vis-à-vis* the international, supranational, and national legal orders. In the following section we will assess the external reach of interoperability according to Article 50 of Regulation (EU) 2019/817 and Regulation (EU) 2019/818 which regulate the 'communication' of personal data to third parties⁴. According to this norm:

'Without prejudice to Article 65 of Regulation (EU) 2018/1240, Articles 25 and 26 of Regulation (EU) 2016/794, Article 41 of Regulation (EU) 2017/2226, Article 31 of Regulation (EC) No 767/2008, and the querying of Interpol databases through the ESP in accordance with Article 9(5) of this Regulation which comply with the provisions of Chapter V of Regulation (EU) 2018/1725 and Chapter V of Regulation (EU) 2016/679, personal data stored in, processed or accessed by the interoperability components shall not be transferred or made available to any third country, to any international organisation or to any private party'.

¹ Paul De Hert, *What are the risks and what guarantees need to be put in place in view of interoperability of police databases?*, IP/C/LIBE/FWC/2005-25, Brussels, 1.02.2006, p. 5.

² Paul De Hert and Serge Gutwirth, *op. cit.*, p. 5.

³ John Palfrey and Urs Gasser, *op. cit.*, p. 11.

⁴ Article 50 of the IO Regulations refer to third countries, international organisations, and private parties. However, our research excludes the latter group under the assumption that the interoperability of the Union large-scale IT systems with private parties will be mainly addressed to airline companies which requires amendments of the PNR and API regulations as we noted in the previous Chapter.

Article 50 of the IO Regulations establishes that the communication of personal data to third countries and international organisations is, in principle, prohibited. Yet, numerous derogations to this prohibition question the rule-exception relationship laid out in Article 50. From these derogations we understand that the external dimension of interoperability must be constructed in two layers. First of all, the interoperability's external dimension relies on each large-scale IT systems' regulation and, specifically, on:

- Article 31 of the revised VIS Regulation;
- Article 41 of the EES Regulation, and
- Article 65 of the ETIAS Regulation.

Provided that the rules on the communication of personal data foreseen in the legislation of large-scale IT systems share common patterns, instead of individually analysing each disposition, we propose a logical-systemic interpretation of the relevant legislations, which we expect to be more fruitful in providing constructive criticism. The specificities of each large-scale IT system will be highlighted as these contribute to the establishment of “global interoperability” in different ways, according to the underlying Union policies and the correspondent objectives pursued. Although the IO Regulations do not refer to the SIS⁵, the Eurodac⁶, and the ECRIS-TCN⁷, these large-scale IT systems have their own external dimension and will be analysed under the assumption that the co-legislators should have inserted them under Article 50 of Regulation (EU) 2019/818. We believe that Article 50 would allow the interconnection of the Union's large-scale IT systems and interoperability components⁸ with third countries' and international organisations' databases. The possibility to directly interconnect a third party's system is expressly envisaged in Articles 9(5) and 50 of the IO Regulations as far as Interpol's SLTD and TDAWN databases are concerned.

The second layer of which the external dimension of interoperability should be constructed is based on the Union's agencies' external actions. Among its exceptions, Article 50 of the IO Regulations refers to Europol – namely Articles 25 and 26 of the Europol Regulation – while making no mention of other freedom, security and justice agencies that are also granted access to the large-scale IT systems and the interoperability components. This legislative choice suggests that the EIS is another candidate for global interoperability. However, and although

⁵ Article 15 of Regulation (EU) 2018/1860; Article 50 of Regulation (EU) 2018/1861, and Article 65 of Regulation (EU) 2018/1862.

⁶ Article 35 of the 2013 Eurodac Regulation.

⁷ Article 18 of the ECRIS-TCN Regulation.

⁸ Probably to the CIR according to the analysis we made in the previous Chapter, yet it would have been preferrable that the co-legislators made it explicit. It is not pacific, then, which personal data are here at stake: will the MID-colored links be shared too?

not directly interconnected, the transfer of personal data toward third countries and international organisations by other Union bodies will also require a certain degree of interoperability, at least as far as data legibility is concerned⁹. Freedom, security and justice agencies have been increasingly delegated the task of processing information, including personal data stored in their own databases or by large-scale IT systems, in light of the progressive datification and technologicalisation of public administrations¹⁰, which suggests that three operational agencies should be considered: Eurojust¹¹; EBCG Agency¹², and EUAA¹³. Thus, we will inspect whether, and under which terms, their external activity justifies the establishment of interoperable solutions in the light of the principles underpinning the transfer and protection of personal data read in respect of the delegation doctrine.

The current Chapter questions the lawfulness of the regime on the communication of personal data to third countries and international organisations set forth in Article 50 of the IO Regulations and/or its consistency with the data protection rules and principles the EU must respect while acting externally. It assesses on what basis personal data is transferred to third parties – whether through an adequacy decision, appropriate safeguards, or derogation clauses – and its compatibility with: on the one hand, the GDPR and the LED as well as the EUDPR for national authorities and Union staff respectively; and, on the other hand, EU primary law enshrining key data protection principles in the exercise of the EU external (implied) competence based on Article 16 of the TFEU and Article 8 of the CFREU.

⁹ John Palfrey and Urs Gasser, *op. cit.*, p. 7: ‘There are degrees and types of interop, which fall along a multidimensional spectrum’.

¹⁰ Marcello Carammia, Stefano Maria Iacus, and Teddy Wilkin, “Forecasting asylum-related migration flows with machine learning and data at scale”, *Scientific Report*, 2022, pp. 1-16.

¹¹ Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, PE/37/2018/REV/1, *OJ L* 295, 21.11.2018, pp. 138-183 (Eurojust Regulation hereinafter).

¹² 2019 EBCG Agency Regulation.

¹³ Regulation (EU) 2021/2303 of the European Parliament and of the Council of 15 December 2021 on the European Union Agency for Asylum and repealing Regulation (EU) No 439/2010, PE/61/2021/REV/1, *OJ L* 468, 30.12.2021, pp. 1-54 (EUAA Regulation hereinafter).

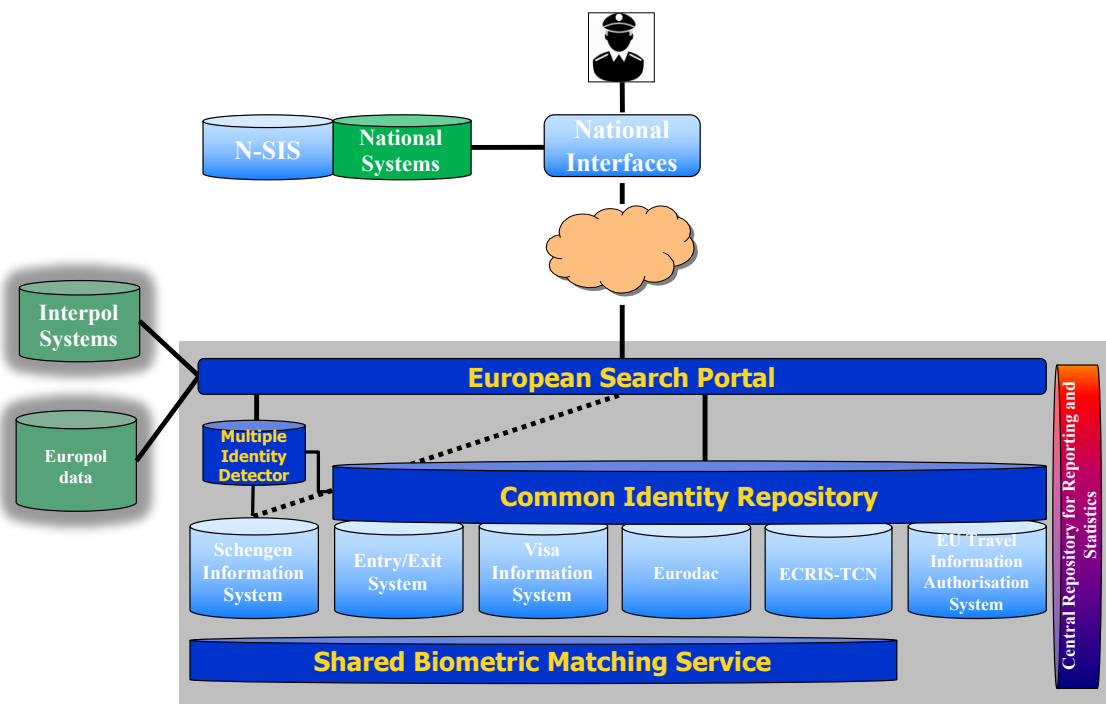


Figure 15 The final picture - Source: Own elaboration from the author's time working at the European Commission.

1. Global interoperability in the Area of Freedom, Security and Justice

1.1. The external dimension of large-scale IT systems

The transfer of personal data to third countries, international organisations and (eventually)¹⁴ private parties or entities is, as a general rule, forbidden in the SIS¹⁵, the VIS¹⁶, the Eurodac¹⁷, the EES¹⁸, the ETIAS¹⁹, and the ECRIS-TCN²⁰. Such a prohibition is justifiable in the light of the Member States' reticence in losing control over the information they hold and in releasing slices of their sovereign power. In this sense, the discourse on the protection of personal data has been instrumentalised to restrict the flow of information, at least where normative standards have not been harmonised²¹. The possibility for transferring the data stored in the systems was

¹⁴ They are expressly mentioned in Articles: 41 of the EES Regulation; 65 of the ETIAS Regulation, and 35 of the 2013 Eurodac Regulation.

¹⁵ Article 50 of Regulation (EU) 2018/1861, Article 65 of Regulation (EU) 2018/1862, and Article 18 of the ECRIS-TCN Regulation.

¹⁶ Article 31(1) of the revised VIS Regulation. Note that the revised VIS Regulation significantly modifies the regime on the 'communication' of personal data to third countries and international organisations while merging the dispositions of the VIS Regulation and the VIS LEA Decision.

¹⁷ Article 35(1) of the 2013 Eurodac Regulation. This prohibition also applies if the data are further processed at national level or between Member States within the meaning of Article 2(b) of the DPF.

¹⁸ Article 41(1) of the EES Regulation.

¹⁹ Article 65(1) of the ETIAS Regulation.

²⁰ Article 18 of the ECRIS-TCN Regulation.

²¹ See Chapters I and II.

advanced as part of the negotiations on the second generation SIS²² and on the VIS Regulation²³, though the exchange of data with third parties was believed to be incompatible with Article 66 of the 1997 TEC, which was only binding for the Member States and the European Commission's administrations²⁴. This topic was discussed on the basis of three options that contemplated its total prohibition, the establishment of adequate guarantees, and the application of national law alone²⁵. Given the European Parliament's opposition and the lack of any transfer disposition in the first generation SIS, the Presidency highlighted that the provision of a general prohibition was the preferable option, and that it would have not impeded the transferring of data under national law²⁶. On that occasion, the EDPS found that '[...] the very possibility of transmitting information to those third parties – which would be a decision falling in any case within the scope of competence of the individual Member States and only apply to the data owned by them, given the system configuration – does not appear to be in line with the purposes of the system as it is currently configured'²⁷.

Yet, the opportunity to forward data to third countries and international organisations to prove the identity of migrants turned out to be an attractive solution in the fight against illegal entries and Member States finally agreed to “open the frontlines” of large-scale IT systems²⁸. Given that the Member States' national law on data protection was harmonised under the DPD and the DPF, Member States agreed that the common principles established therein were sufficiently reassuring so as to allow the transfer of data to third countries, subject to the consent

²² See the discussions on Article 48 in the Council of the EU, *Transfer of personal data to third parties: Article 48 of the Council Decision on the establishment, operation and use of the second generation Schengen Information System (SIS II)*, 14092/05, Brussels, 9 December 2005.

²³ See the Council of the EU, *Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences – Bridging Clause*, 8803/07, Brussels, 14 April 2007.

²⁴ See the Council of the EU, *Draft Conclusions on the development of the Visa Information System (VIS)*, 6010/04, Brussels, 9 February 2004, p. 2.

²⁵ See the Council of the EU, *Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences – proposals for re-drafting*, 14196/1/06, Brussels, 23 November 2006.

²⁶ See the Council of the EU, *Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences – Bridging Clause*, 8803/07, Brussels, 14 April 2007, and the Council of the EU, *Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences – proposals for re-drafting*, 14196/1/06, Brussels, 23 November 2006.

²⁷ See the Council of the EU, *Opinion of the European Data Protection Supervisor on the legislative proposals concerning the Second Generation Schengen Information System (SIS II)*, 14091/05, Brussels, 14 November 2005, p. 15.

²⁸ See Article 31 of the VIS Regulation.

of the data owner and according to the internal law of the State concerned. As a result, the possibility of transferring data to a third country was tied to the need to prove the identity of third-country nationals, including for the purposes of return, only when: the European Commission had adopted an adequate decision on the third country to which the data was being transferred; the third country agreed to use the data only for the purpose specified in the transfer, and the Member State that entered the data gave its consent. Each State would maintain control over its own data, despite the fact that it was made available to other Member States, since any transfer of data to third parties by a Member State other than the one that had entered the data in the system was subjected to the prior consent of the latter. Only in case of serious and imminent threat could the data have been transferred without seeking the permission of the Member State holding the data. Thus, the communication of personal data stored in large-scale IT systems has been regulated by a legislation of exception that can be divided into two main groups of rules:

- a first set of rules that goes back to the GDPR and Chapter V of the EUDPR to regulate the transfer of personal data based on the “freedom” section, and
- a second set of rules that takes as a point of reference the LED and Chapter IX of the EUDPR as far as PJCCM are concerned.

1.1.1. The communication of personal data to facilitate the return of irregular migrants and resettle third country nationals

In the cases of the SIS²⁹, the VIS³⁰, the EES³¹, the ETIAS³², and the Eurodac³³, personal data³⁴ may be accessed by competent authorities³⁵ and transferred or made available to third parties, provided that ‘it is necessary in individual cases in order to prove the identity of third-country nationals’³⁶. Specifically, identification may be required when:

- returning the third-country national for which purposes personal data was transferred or disclosed to a third country or international organisation by the SIS³⁷, the VIS³⁸, the EES³⁹, and the ETIAS⁴⁰, or

²⁹ Article 15(1) of Regulation (EU) 2018/1860.

³⁰ Article 31(2) of the VIS revised Regulation refers to personal data of short-stay visa applicants in Article 9(4)(a), (b), (ca), (k) and (m), and Article 9(6) and (7), and specifically to: surname (family name); first name(s) (given name(s)); date of birth; current nationality or nationalities; sex; the type and number of the travel document; the country which issued the travel document and its date of issue; residence; in the case of minors, surname and first name(s) of the applicant's father and mother; fingerprints of the applicant, in accordance with Article 13 of the Visa Code, a scan of the biographic data page of the travel document. As far as long-stay visa or residence permits are concerned, instead, Article 22a(1)(d) to (i) and (k) contemplates the following data: surname (family name); first name(s) (given name(s)); date of birth; current nationality or nationalities; sex; the type and number of the travel document; the country which issued the travel document and its date of issue; residence; in the case of minors, surname and first name(s) of the applicant's father and mother; fingerprints of the applicant, in accordance with Article 13 of the Visa Code, a scan of the biographic data page of the travel document.

³¹ Article 41(2) of the EES Regulation refers to border authorities or immigration authorities.

³² Article 65(3) of the ETIAS Regulation refers to immigration authorities only.

³³ Articles 35(2) and 35(3) of the 2013 Eurodac Regulation allow the transfer of personal data: first, if they have been previously exchanged among Member States following a Eurodac hit and there is no ‘a serious risk that as a result of such transfer the data subject may be subjected to torture, inhuman and degrading treatment or punishment or any other violation of his or her fundamental rights’; second, to third countries to which the 2013 Eurodac Regulation applies – i.e., Iceland, Liechtenstein, Norway, and Switzerland.

³⁴ In the case of SIS, Article 15(1) of the Regulation (EU) 2018/1860 only refers to some categories of data and the related supplementary information, that are those referred to in points (a), (b), (c), (d), (e), (f), (g), (h), (q), (r), (s), (t), (u), (v) and (w) of Article 4(1), namely: surnames; forenames; names at birth; previously used names and aliases; place of birth; date of birth; gender; any nationalities held; the category of the person's identification documents; the country of issue of the person's identification documents; the number(s) of the person's identification documents; the date of issue of the person's identification documents; photographs and facial images; dactyloscopic data, and a copy of the identification documents, in colour wherever possible.

³⁵ Note that in the case of Article 65 of the ETIAS Regulation, immigration authorities must conduct a prior search in the EES in accordance with Article 26 of the EES Regulation, so that the access to the ETIAS is allowed when this search indicates that the EES does not contain data concerning the third-country national to be returned. Article 26 of the EES Regulation allows immigration authorities to access the EES to verify through a biometric one-to-one comparison the identity of the third-country national, or checking or verifying whether the conditions for entry to, or stay on, the territory of the Member States are fulfilled, or both.

³⁶ Article 15 of the Regulation (EU) 2018/1860 states that the transfer or disclosure of personal data may serve for the issuance of an identification or travel document of an illegally staying third-country national in view of his or her return – see, for example, Sergio Carrera, 2016, *op. cit.*

³⁷ Article 15(1) of the Regulation (EU) 2018/1860.

³⁸ Article 31(2) of the VIS revised Regulation.

³⁹ Article 41(2) of the EES Regulation.

⁴⁰ Article 65(3) of the ETIAS Regulation.

- in the case of the VIS, resettling a third country national in accordance with European⁴¹ or national schemes⁴².

Data can be communicated – i.e., transferred or disclosed – to third countries and/or one of the international organisations listed in the corresponding Annexes⁴³ for the purpose of ‘proving the identity’ of the third-country national. These organisations are: UN organisations (such as the UNHCR)⁴⁴; the International Organisation for Migration (IOM)⁴⁵, and the International

⁴¹ Commission Recommendation (EU) 2020/1364 of 23 September 2020 on legal pathways to protection in the EU: promoting resettlement, humanitarian admission and other complementary pathways, C(2020) 6467, *OJ L* 317, 1.10.2020, pp. 13-22. On resettlement see, for example, Janine Prantl, “Shaping the Future Towards a Solidary Refugee Resettlement in the European Union”, *European Papers*, Vol. 6, No. 2, 2021, pp. 1027-1048.

⁴² Article 31(2) of the revised VIS Regulation.

⁴³ Article 15 of the Regulation (EU) 2018/1860 refers to third countries only. In the specific case of resettlement, the VIS data can actually be transferred to an international organisation only and not to third countries, which conforms with the FRA comments urging not to transfer personal data until the whole procedure is completed – see FRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Brussels, 27.03.2018, p. 14.

⁴⁴ See: Guy S. Goodwin-Gill, “The Office of the United States High Commissioner for Refugees and the Sources of international Refugee Law”, *International and comparative law quarterly*, Vol. 69, No. 1, 2020, pp. 1-41; Enrico Massa, “L’evoluzione del diritto internazionale dei rifugiati attraverso la partecipazione dell’ACNUR alla funzione giurisdizionale”, *La Comunità Internazionale: rivista trimestrale della Società Italiana per l’Organizzazione Internazionale*, Vol. 74, No. 3, 2019, pp. 419-445; Ellen Reichel, “Navigating between refugee protection and state sovereignty: legitimating the United Nations High Commissioner for Refugees”, in Laus Dingwerth, Antonia Witt, Ina Lehmann, Ellen Reichel, and Tobias Weise, *International organizations under pressure: legitimating global governance in challenging times*, Oxford, Oxford University Press, 2019, pp. 195-231; Sarah Deardorff Miller, *UNHCR as a surrogate state: protracted refugee situations*, London/New York, Routledge/Taylor and Francis Group, 2018, and T. Alexander Aleinikoff, “The Mandate of the Office of the United Nations High Commissioner for Refugees”, in Vincent Chetail and Céline Bauloz, *Research handbook on international law and migration*, Cheltenham, UK/US, Edward Elgar Publishing, 2014, pp. 389-416. On the relationship between the EU and the UNHCR and the IOM see Julinda Beqiraj, Jean-Pierre Gauci, and Anna Khalfaoui, “United Nations High Commissioner for Refugees (UNHCR) and International Organization for Migration (IOM)”, in Ramses A. Wessel and Jed Odermatt, *Research Handbook on the European Union and International Organizations*, Cheltenham, Edward Elgar Publishing, 2019, pp. 222-239, highlighting how Declaration No 17 on Article 73k of the Treaty of Amsterdam foresaw that the European Community should have consulted the UNHCR and other relevant international organisations for asylum matters.

⁴⁵ See, for example: Elspeth Guild, Stefanie Grant and C A Groenendijk, “Unfinished Business: the IOM and Migrants’ Human Rights”, in Martin Geiger and Antoine Pécoud, *The International Organization for Migration: the new ‘UN Migration Agency’ in critical perspective*, Cham, Palgrave Macmillan, 2020, pp. 29-52; Megan Bradley, *The international organization for migration: challenges and complexities of a rising humanitarian actor*, London, Routledge, 2015; Manuel Pombo, *La realidad migratoria y las políticas migratorias : la organización internacional para las migraciones*, Madrid, Dykinson, 2012; Alberto Giovanetti Ramos, “Inmigrantes en situación irregular y la Organización Internacional para las Migraciones”, in Angel G. Chuenca Sancho, *Derechos Humanos, inmigrantes en situación irregular y Unión Europea*, Valladolid, Lex Nova, 2010, pp. 97-111, and Kevin In-Chuen Koh, “International Organisation for Migration”, in Christian Tietje and Alan Brouder, *Handbook of transnational economic governance regimes*, Leiden, Nijhoff, 2009, pp. 191-200.

Committee of the Red Cross (ICRC)⁴⁶. In the case of the SIS⁴⁷, the VIS⁴⁸, the EES⁴⁹, and the ETIAS⁵⁰, the transfer or availability of personal data must be legitimised by the following:

- the European Commission has adopted a decision on the adequate level of protection of personal data in the third country or international organisation in question in accordance with Article 45(3) GDPR;
- appropriate safeguards have been provided according to Article 46 GDPR, such as through a readmission agreement in force between the Union or a Member State and the third country in question, or
- when Article 49(1)(d) GDPR⁵¹ applies⁵².

Therefore, interoperability with foreign systems will not always be limited to *ad hoc* transfers or specific cases with regard to the availability of data, as Prof. De Hert and Prof. Gutwirth wished. Conversely, the flow of information depends on the applicability of the EU regime on the protection of personal data. Besides, the SIS⁵³, the VIS⁵⁴, the EES⁵⁵, and the ETIAS⁵⁶ establish that the following conditions must be respected:

- the transfer of data must be carried out in accordance with the relevant provisions of Union law, in particular the provisions on data protection (including Chapter V of the GDPR), readmission agreements, and the national law of the Member State transferring the data;
- the third country or international organisation has agreed to process the data only for the purposes for which it was provided, and

⁴⁶ See the Annex attached to the VIS Regulation.

⁴⁷ Article 15(2) of the Regulation (EU) 2018/1860: ‘The transfer of the data to a third country shall be carried out in accordance with the relevant provisions of Union law, in particular provisions on protection of personal data, including Chapter V of Regulation (EU) 2016/679, with readmission agreements where applicable, and with the national law of the Member State transferring the data’.

⁴⁸ Article 31(2) of the revised VIS Regulation.

⁴⁹ Article 41(2) of the EES Regulation.

⁵⁰ Article 65(3), fourth paragraph, of the ETIAS Regulation.

⁵¹ That is: ‘the transfer is necessary for important reasons of public interest’.

⁵² Article 15(6) of the Regulation (EU) 2018/1860 specifies that: ‘Application of Regulation (EU) 2016/679, including with regard to the transfer of personal data to third countries pursuant to this Article, and in particular the use, proportionality and necessity of transfers based on point (d) of Article 49(1) of that Regulation, shall be subject to monitoring by the independent supervisory authorities referred to in Article 51(1) of that Regulation’.

⁵³ Article 15(3) of Regulation (EU) 2018/1860.

⁵⁴ Article 31(3) of the VIS revised Regulation.

⁵⁵ Article 41(3) of the EES Regulation.

⁵⁶ In the case of the ETIAS, these conditions are valid only for the data referred to in Article 17(2)(a), (aa), (b), (d), (e) and (f). These data are: surname (family name), first name(s) (given name(s)), surname at birth; date of birth, place of birth, sex, current nationality; country of birth, first name(s) of the parents of the applicant; other names (alias(es), artistic name(s), usual name(s)), if any; type, number and country of issue of the travel document; the date of issue and the date of expiry of the validity of the travel document, and the applicant’s home address or, if not available, his or her city and country of residence.

- if a return decision adopted pursuant to the Return Directive has been issued in relation to the third-country national concerned, its enforcement must not be suspended, and no appeal can have been lodged which may lead to the suspension of its enforcement.

A further requisite is foreseen in the case of the SIS⁵⁷ and of the VIS⁵⁸, for which the Member State that entered the data must give its approval for any transfer or disclosure performed by another Member State. Regrettably, only the SIS specifies that the third-country national concerned must be informed that their personal data and supplementary information may be shared with the authorities of a third country⁵⁹. These risks hampering the data subject's right to information while legitimising the disclosure of personal data to third parties by virtue of the public policy exception underpinned by Article 46(1)(d) GDPR. A final clause makes safe 'the rights of applicants for and beneficiaries of international protection, in particular as regards non-refoulement'⁶⁰. That is, personal data must not be communicated or made available to third countries or international organisations if the person concerned risks being subjected to torture and inhumane and degrading treatment or punishment.

a) Interoperability with third countries

According to Chapter V of the GDPR, the transfer of personal data can be based on: adequacy decisions; appropriate safeguards, or derogation clauses⁶¹. As we advanced in

⁵⁷ Article 15(1) of Regulation (EU) 2018/1860.

⁵⁸ Article 2(b), second paragraph, of the VIS revised Regulation.

⁵⁹ Article 15(3)(b) of Regulation (EU) 2018/1860.

⁶⁰ See: Article 15(4) of the Regulation (EU) 2018/1860 that refers to Article 30 of the Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection, *OJL* 180, 29.6.2013, pp. 60-95; Article 31(3) of the VIS revised Regulation; Article 41(4) of the EES Regulation, and Article 65(4) of the ETIAS Regulation. Article 35(2) of the 2013 Eurodac Regulation implicitly refers to it while stating that: 'Personal data which originated in a Member State and are exchanged between Member States following a hit obtained for the purposes laid down in Article 1(2) shall not be transferred to third countries if there is a serious risk that as a result of such transfer the data subject may be subjected to torture, inhuman and degrading treatment or punishment or any other violation of his or her fundamental rights'. The principle of *non-refoulement* or prohibition of *refouler* prevents states from removing persons who may be subjected to torture and inhuman or degrading treatment in their country of origin or of previous residence. It was enshrined for the first time in the Convention Relating to the Status of Refugee as amended by the Protocol relating to the Status of Refugees, *U.N.T.S.*, No. 8791, Vol. 606, p. 267, signed in New York on 31 January 1967, and entered into force on 4 October 1967. On the principle of non-refoulement see: James C. Hathaway, *The rights of disputes under international law*, Cambridge, Cambridge University Press, 2018; Guy S. Goodwin-Gill, "Non-Refoulement in the 1951 Refugee Convention" in Guy S. Goodwin-Gill, *The refugee in International Law*, Oxford, Clarendon Press, 2007, pp. 201-284; Francesco Salerno, "L'obbligo internazionale di non-refoulement dei richiedenti asilo" in Chiara Favilli, *L'obbligo internazionale di non-refoulement dei richiedenti asilo*, Italy, Cedam, 2011, pp. 1-33, and Id., "L'obbligo internazionale di non-refoulement dei richiedenti asilo", *Diritti umani e diritto internazionale*, No. 3, 2010, pp. 487-515.

⁶¹ In this specific case Article 49(1)(d) of the GDPR.

Chapter II, these tools require different expedients following an examination of the level of protection ensured by the third party.

In the absence of an adequacy decision, the data stored in the SIS, the VIS, the EES, and the ETIAS, can be transferred or made available on the basis of appropriate safeguards, among which, as we shall highlight, are legally binding, enforceable instruments. The fact that readmission agreements are simply equated to appropriate safeguards is a questionable practice if we consider that, from a human rights perspective, the enforceable character of the data protection rules agreed therein has not been assessed⁶². As of today, the EU has concluded seventeen readmission agreements regarding irregular migrants⁶³ and, as a result, it is now recognised an express external competence⁶⁴. All European readmission agreements include a data protection clause that consists of two main parts, namely an introductory *chapeau* and a set of core principles.

Given that the term ‘transfer of personal data’ used in EU legislation has not been defined, it can be argued that this concept includes what the European readmission agreements’ clause describes as ‘communication’ of data. The clause states that data must be transferred between the ‘competent authorities’ of the third country and the Member States – e.g., excluding EU agencies⁶⁵. These stipulations are laid down in unpublished implementing Protocols and it is not possible to know *a priori* which categories of authorities are accountable for the processing of personal data. Specifically, the data subject should be informed of the identity and contact details of the data controller according to Articles 13(1)(a) and 14(1)(a) of the GDPR in order to raise an appeal against them⁶⁶. In addition, no definition of ‘processing’ is given, and it is not clear how it differs from the expression ‘treatment of personal data’. The laws applicable to the processing of personal data are, respectively, those of the third country and those of the EU Member State in question, the latter having been harmonised by the DPD. Since the GDPR establishes the current level of protection, the reference to the Member State’s internal legislation should be replaced by a new one referring to the GDPR.

⁶² See Chapter II.

⁶³ The Regulation (EU) 2018/1860, and the VIS, the EES, and the ETIAS Regulations refer to readmission agreements in general terms so also those concluded by the Member States are contemplated being it a shared external express competence underpinned by Article 79(3) TFEU – see Paula García Andrade, 2015, *op. cit.*, p. 333 ff.

⁶⁴ Articles 78(2)(g) and 79(3) TFEU. This paragraph is extracted from the contribution of Francesca Tassinari, “Privacy enhancing readmission: the clause on data protection in the EURAs”, *ADiM Blog, Analyses & Opinions*, 30.06.2021, available at www.adimblog.com.

⁶⁵ Usually to the so-called “Readmission Case Management Systems” that the European Commission financed in the frame of the EU Readmission Capacity Building Facility – see the IOM, *European Readmission Capacity Building Facility – EURCAP*, available at <https://eea.iom.int>.

⁶⁶ Article 79 GDPR.

In its body, the European readmission agreements' clause lists a set of norms recalling numerous data protection principles which we welcome. Yet, some criticism can still be raised. First, recalling two of the essential elements listed under Article 8(2) CFREU, the clause states that personal data must be processed fairly and lawfully. Second, it sets forth that personal data must be collected for the specified, explicit, and legitimate purpose of implementing the European readmission agreements and not be further processed by the communicating or receiving authority in a way incompatible with that purpose. The principle of purpose limitation is a cornerstone of the fundamental right to the protection of personal data, but it is not absolute⁶⁷. Thus, in the overall framework of how data flows between third countries and international organisations, it may be advisable to oblige the parties to authorise each other to process personal data for further compatible purposes within the limits enshrined in Article 6(4) GDPR.

Third, personal data must be adequate, relevant, and not excessive in relation to the purpose for which it is collected and further processed. Although not embedded in Article 8 CFREU, the principle of data minimisation integrates the strict necessity test deployed under Article 52(1) CFREU and is a crucial feature for assessing the legality of the transfer operation⁶⁸. Specifically, the categories of data communicated shall be specified, and so do the European readmission agreements' clause and the annexes to the agreements. The same rationale underpinning the purpose limitation principle applies to storage limitation. The clause states that personal data must be kept in a form which permits the identification of the data subject for no longer than is necessary for the purpose for which the data was collected or was further processed. However, the specification of a maximum data retention period would fulfil the requirements found in Article 52(1) CFREU.

Besides, the European readmission agreements' clause foresees that data shall be kept accurate and, where necessary, up-to-date, in line with the individual's right to access and rectify data as recognised by the CFREU. The clause maintains that both the communicating and the receiving authority shall take every reasonable step to ensure, as appropriate, the rectification, erasure, or blocking of personal data where the processing does not comply with the provisions of the Article. This provision is particularly relevant if the data is not adequate, relevant, or accurate, or if it is excessive in relation to the purpose of the processing. Besides, the European readmission agreements' clause establishes that competent authorities shall notify

⁶⁷ See Chapter I.

⁶⁸ *Ibidem*.

the other contracting party of any rectification, erasure, or blocking, which is consistent with the EDPB's guidelines⁶⁹.

Some duties surrounding the principle of the confidentiality and security of data can be inferred from the communication of personal data is restricted to the competent authorities alone, while imposing the prior consent of the communicating authority if further communications are to be made to other bodies. This rule acquires an added value with regard to the so-called "onward transfer" that shall be subjected to the same principles and safeguards as the first transfer with respect to the purpose limitation principle. Onward transfers shall be subject to the prior and express authorisation of the transferring body and should be recorded and made available to the data protection authority, if necessary. In this regard, the wording of the European readmission agreements' clause should be more trenchant in extending the reach of EU protections to other recipients. Moreover, no explicit mention is made of the principle of security and the need to cooperate in the case of a data breach. Article 4(12) GDPR obliges the controller to inform the data subject of the serious risks stemming from a data breach, including when this is the result of a security incident. Finally, although we welcome the insertion of a disposition binding the communicating and receiving authorities to keep a written record of the communication and a receipt regarding the personal data, the principle of accountability might have been enhanced by requiring the submission of such reporting to the corresponding supervisory authority.

Further safeguards might have been inserted, such as the prohibition of decisions fully based on ADM and of the transferring of 'special categories of personal data', such as biometrics. The European readmission agreements rely on biometrics to identify individuals derogating from the general prohibition set forth by the GDPR⁷⁰. As a result, enhanced safeguards should be added including, for example, the assurance that experts are involved in the enrolment phase. It is not clear why the European readmission agreements' clause affirms that 'upon request, the receiving authority shall inform the communicating authority of the use of the communicated data and of the results obtained therefrom'. If the data is only to be used for the purposes of readmitting migrants to the state of origin or transit, why should the receiving authority not communicate the result of the use of the communicated data?

Regrettably, the European readmission agreements' clause does not foresee any provision either regarding data protection authorities or the enforceability of the data subject's recognised

⁶⁹ Guidelines of the EDPB No. 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies, Brussels, 15.12.2020.

⁷⁰ Article 9 GDPR.

rights. Although the clause requires that the communicating and the receiving authorities take every reasonable step to ensure, as appropriate, the rectification, erasure, or blocking of personal data where the processing does not comply with the relevant agreement, it does not empower the individual *vis-à-vis* public authorities. Conversely, the principle of transparency enables the data subject to gain knowledge of:

- the personal data processing activities the public authorities carry out with their data;
- the relevant tools used for the transfer;
- the entities to which the data may be transferred;
- the rights available to the data subject and the applicable restrictions;
- the existence of available redress mechanisms, and
- the contact details for the submission of a dispute or claim.

The provision of restrictions shall be laid down by law in accordance with Article 23 GDPR in order to prevent the watering down of the rights recognised to the individual. The EDPB urges⁷¹ the contracting parties to publish the agreement and provide a summary in order to clarify its contents. It also suggests that if one of the two parties does not comply with the agreements, the transferred data will be returned or deleted by the receiving authority, and the data protection authority will be notified.

Recalling Article 46(1) GDPR, the norm demands that the controller or processor in charge of transferring personal data on the basis of appropriate safeguards to assess whether ‘enforceable data subject rights and effective legal remedies for data subjects are available’⁷². According to the Article, the data subject must be afforded access to redress mechanisms if foreign authorities do not comply with the agreed provisions. The GDPR guarantees not only the right to a judicial remedy in full respect of Article 47 CFREU, but also the right to compensation in case harm is caused⁷³. If a judicial remedy is not guaranteed, the EDPB recommends ensuring the availability of alternative safeguards – e.g., arbitration, alternative dispute resolution, or mechanisms implemented by international organisations. As we have analysed elsewhere, the EU promotes “enforceability” through bottom-up mechanisms – e.g., national supervisory authorities that are called on to ensure the compliance with data protection principles – and through normative standards agreed multilaterally – first of all, by promoting adherence to Convention 108 of the Council of Europe. As a result, the oversight authority of

⁷¹ Guidelines of the EDPB No. 2/2020 on *articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies*, Brussels, 15.12.2020.

⁷² See Chapter II.

⁷³ Article 82 GDPR.

the receiving state should be called on to cooperate with EU data protection authorities while monitoring bodies can induce a third country to comply with agreements on international human rights.

At first sight, the European readmission agreements' clause does not comply *per se* with Article 46(1) GDPR unless the third country ensures further guarantees – e.g., in the unpublished implementing Protocols mentioned *supra*, or in the practical implementation of the agreements – the nature of which is not known to us. If it is true that appropriate safeguards impose on the controller the obligation to assess the “adequacy” of the third country’s legislation⁷⁴, we believe that, because of its vagueness and lack of sufficient guarantees, the European readmission agreements' clause risks overburdening the authorities in question, which may not have the means to assess the suitability of the third country’s legislation. Also, the additional requisite set forth by the system’s regulations, consisting of the need for the third country to agree to process data only for the purposes for which it was provided, is a positive guarantee, yet not sufficient: What are the terms in which such an agreement would be formalised? Who is going to supervise the third party’s commitment to the agreement? And what are the juridical consequences in case of non-compliance? We believe that there are serious doubts as to the “appropriateness” of this clause suggesting that, in reality, readmission agreements must not be considered as a valid legal basis to transfer personal data. If so, the flow of information between the EU and such a third country would result to be regulated by derogation clause – i.e., *ad hoc* transfers – more than a “legally binding enforceable instrument”.

b) Interoperability with international organisations

The regimes on the transfer or availability of personal data from the SIS, the VIS, the EES, and the ETIAS to international organisations for the purpose of identification⁷⁵ include three main actors: the UNHCR, the IOM, and the ICRC⁷⁶. We should warn that the GDPR systematises these three organisations with the label of “international organisation” without

⁷⁴ For which purpose, the controller is expected to evaluate for and foremost the adherence or not of the third country to the Convention 108.

⁷⁵ For a critic, see Mark Latonero, Keith Hiatt, Antonella Napolitano, Giulia Clericetti, and Melanie Penagos, *Digital Identity in the Migration & Refugee Context: Italy Case Study*, Italy, 2019, available at www.datasociety.net.

⁷⁶ Other partnerships contemplated in “Un budget humanitaire solide et flexible, une priorité du Parlement européen pour l'action humanitaire future de l'UE”, *Bulletin Quotidien Europe*, No. 12855, 17.12.2021, are United Nations Children's Fund and the Food and Agriculture Organisation.

taking into account their different status under public international law⁷⁷. According to the GDPR, an “international organisation” is ‘an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries’⁷⁸. As we are not aiming to dwell on this questionable, wide definition, we shall limit ourselves to pointing out that such a broad concept of what constitutes an international organisation could generate uncertainty when assessing the range of the agreement concluded between the EU and the other actor. Notwithstanding the label used by the GDPR, we hereby recall that only states have, and international organisations may be⁷⁹, provided with international legal capacity. Therefore, only when the party with which the EU undertakes negotiations is recognised as having international subjectivity, then, we can state with certainty that an international agreement, or a treaty, can be concluded under public international law⁸⁰.

⁷⁷ The UNHCR is a secondary organ created by the UN with the Resolution of the General Assembly No. A/RES/428(V) of 14 December 1950, *Statute of the office of the United Nations high commissioner for refugees*, on the basis of the 1951 Geneva Convention. Therefore, the UNHCR is a UN secondary body established by a principal one and not an international organisation.

⁷⁸ See recital (26) of the GDPR. The IOM can be classified as a UN specialised organisation. Finally, the possibility to include the ICRC is given by the last sentence referring to ‘an agreement between two or more countries’. See Christopher Kuner, “International Organizations and the EU General Data Protection Regulation”, *International Organization Law Review*, No. 16, 2019, pp. 158-191.

⁷⁹ Article 6 of the Vienna Convention on the Law of Treaties between States and International Organizations or between International Organizations signed in Vienna on 21 March 1986, not yet entered into force, rules that: ‘The capacity of an international organization to conclude treaties is governed by the rules of that organization’. Unfortunately, international subjectivity is seldomly expressed in the constitution of international organisations and their legal capacity is interpreted on the basis of the doctrine on implied powers that takes knowledge of the ‘rules’ sets forth under Article 2(1)(j) of the Vienna Convention on the Law of Treaties of 21 March 1986. On the topic, see: José Antonio Pastor Ridruejo, *op. cit.*, p. 70 ff.; Manuel Díez de Velasco Vallejo, *op. cit.*, p. 64 ff., and Sobrino Heredia, *op. cit.*, pp. 346-370.

⁸⁰ Article 2(1)(a) of the Vienna Convention on the Law of Treaties of 21 March 1986.

The UNHCR and the IOM are considered as “implementing partners”⁸¹ of the Global Approach to Migration and Mobility for which purpose they (arguably)⁸² receive EU funding⁸³. In practice, these two organisations contribute to the implementation of the AFSJ within and beyond the EU’s borders. If acting within the Member States’ territories, the UNHCR and the IOM usually operate alongside Member States’ authorities and EU staff, in their external activity they act as protagonists alongside foreign authorities in relocating border controls⁸⁴ while assuming responsibility for analysing asylum applications⁸⁵. Provided that the UNHCR and the IOM activities are operationally deployed in third countries’ territories, their relationship with the EU is configured through two interrelated aspects: first, the delegation doctrine⁸⁶; second, the offshoring of border controls and asylum seeker procedures⁸⁷. This

⁸¹ On the cooperation between the UNHCR and the IOM see: IOM, “UNHCR Adapting to Modern Complexities of Resettlement, Mixed Migration Flows”, *Press Release*, 12.18.2019, available at www.iom.int. From an individual-centred perspective, Lama Mourand, “Transforming refugees into migrants: institutional change and the politics of international protection”, *European Journal of International Relations*, 2019, pp. 1-27, p. 20, finds that by blurring the lines between refugees and migrants, states and international migration bodies gain ‘[...] greater control over how and when individuals qualify for international protection’.

⁸² Unfortunately, the funding chosen by the European Commission are not always directed at pursuing migration and asylum goals as it is the case of the Instrument Contributing to the Stabilisation and Peace and the European Union Emergency Trust Fund financing the Agadez Migration, the Migration Resource and Response Mechanism, and the Sustainable Return from Niger projects that fall within the EU policy on humanitarian aid. In this regard, see Julia Van Dessel, “International Delegation and Agency in the Externalization Process of EU Migration and Asylum Policy: the Role of the IOM and the UNHCR in Niger”, *European Journal of Migration and Law*, 2019, pp. 435-458, and Goran Bandov and Gabrijela Gosovic, “Humanitarian Aid Policies within the European Union External Action”, *Journal of Liberty and International Affairs*, Vol. 4, No. 2, 2018, pp. 25-39, p. 27: ‘[...] the politicization of humanitarian aid occurs when humanitarian aid is used as an instrument of foreign policy in order to achieve internal and external political goals and it results in the violation of international humanitarian law’. Also, you can confront the Council of the EU, *Council Conclusions on taking the UN-EU strategic partnership on peace operations and crisis management to the next level: Priorities 2022-2024*, 5451/22, Brussels, 24 January 2022.

⁸³ See also Julinda Beqiraj, “Strengthening the Cooperation between IOM and the EU in the field of Migration”, in Francesca Ippolito, *Migration in the Mediterranean: mechanisms of international cooperation*, Cambridge, Cambridge University Press, 2015, pp. 115-135; Claire Potaux, “The Current Role of the International Organization for Migration in developing and implementing Migration and Mobility Partnerships”, in Rahel Kunz, Sandra Lavenex, and Marion Panizzon, *Multilayered migration governance: the promise of partnership*, Abingdon, Routledge, 2011, pp. 183-204.

⁸⁴ For example: Entrada en vigor del Acuerdo entre el Reino de España y el Reino de Marruecos relativo a la circulación de personas, el tránsito y la readmisión de extranjeros entrados ilegalmente, hecho en Madrid el 13 de febrero de 1992, *Boletín Oficial del Estado* 299, 13 December 2012, p. 85068; MoU on cooperation in the fields of development, the fight against illegal immigration, human trafficking and fuel smuggling and on reinforcing the security of borders between the State of Libya and the Italian Republic of 2017 available at www.eumigrationlawblog.eu, and EU-Turkey Statement of 18 March 2016 available at www.consilium.europa.eu.

⁸⁵ As it is the case of the Denmark-Rwanda MoU regarding cooperation on asylum and migration issues of 27 April 2021 available at www.minaffet.gov.rw.

⁸⁶ See Chapter IV. In her lecture at The Hague Academy of International Law, *L’externalisation en matière de migrations internationales: aspects juridiques*, The Hague, 24-28 January 2022, Prof. Corneloup defined ‘delegation’ as ‘any act through which a state entrusts another person – state, an organisation or a private individual – with missions in respect of migration’ (the translation is ours).

⁸⁷ Prof. Corneloup, *ibid.*, explains that the term ‘externalisation’ lacks a legal definition – and therefore a legal regime – in international and supranational instruments and originates from economic and management sciences. As stated by José Alejandro del Valle Gálvez, “La fragilidad de los derechos humanos en las fronteras exteriores

phenomenon, also known as ‘outsourcing’ the management of migration and asylum policies⁸⁸, is highly problematic from a human rights perspective⁸⁹ as it builds up walls between the individual and the state of destination⁹⁰ while blurring the lines of the latter’s responsibility when it is “indirectly” acting in foreign lands. The situation is further complicated by the fact that the agent usually subcontracts its own services to private parties. The high level of discretion enjoyed by the UNHCR and the IOM puts into question the validity of the principal/agent relationship with the European Commission and risks being confused with a mere form of practical cooperation that carries no legal consequences. Besides, the UNHCR and the IOM’s action is justified differently *vis-à-vis* EU implementing powers: in the case of the UNHCR⁹¹, the European Commission is delegating its executive powers to support Member States in the recognition of the refugee status to third country nationals in light of the 1951 Geneva Convention obligations, while the IOM has no international mandate in the asylum field⁹².

européas, y la externalización/extraterritorialidad de los controles migratorios”, in Juan Soroeta Licerias and Nicolás Alonso Moreda, *Anuario de los cursos de derechos humanos de Donostia-San Sebastián*, Vol. XVIII, 2019, pp. 25-58, and Id., “Inmigración, derechos humanos y modelo europeo de fronteras. Propuestas conceptuales sobre ‘extraterritorialidad’, ‘desterritorialidad’ y ‘externalización’ de controles y flujos migratorios”, *Revista de Estudios Jurídicos y Criminológicos*, No. 2, Universidad de Cádiz, 2020, pp. 145-210, when we study outsourcing practices in the migration field we should contemplate both the possibility that the state – or the international organisation – acts itself with its own officials abroad (extraterritoriality) and the fact that the state – or the international organisation – entrusts to another party (whether private or public) the execution of its sovereign powers – conferred competences – (externalisation). Prof. Corneloup adds that two different layers should be taken into account: a vertical/private and a horizontal/public ones, though these share common features – i.e., a shift from the inside to the outside, whether with delegation or not – that give rise to common legal issues – i.e., responsibility –, and need similar legal responses – distance between the state and the migrant. However, when it comes to analyse the management of the EU external border, new technologies give birth to a hybrid form of extraterritoriality for which states and international organisations’ authorities and officials can act within the Schengen area territory without counting on third parties’ forces – see, for example, Paul Trattuttmansdoff, “The Politics of Digital Borders”, in Cengiz Günay and Nina Witjes, *Border Politics*, Cham, Springer International Publishing, 2017, pp. 107-126. Interestingly, this option can be included into Prof. Corneloup’s definition of outsourcing as: ‘a shift of a state activity in matters relating to migration activity, from inside to outside, provoking distance between the State and the migrant’ (our own translation).

⁸⁸ Alexander Betts and James Milner, “The Externalization of EU Asylum Policy: The Position of African States”, *Danish institute for international studies*, Copenhagen, 2007.

⁸⁹ Elspeth Guild, Stefanie Grant, and C A Groenendijk, *loc. cit.*

⁹⁰ Simon Robins, “The Affective Border: Missing Migrants and the Governance of Migrant Bodies at the European Union’s Southern Frontier”, *Journal of Refugee Studies*, 2019, pp. 1-19.

⁹¹ Article 35 of the 1951 Geneva Convention and Article II of its 1967 Protocol oblige the states parties – among which all the EU Member States – to cooperate with the UNHCR in the exercise of its mandate, in particular facilitating UNHCR’s duty of supervising the application of the provisions of the 1951 Geneva Convention and its 1967 Protocol. Article 78(1) TFEU establishes that the EU common policy on asylum, subsidiary protection and temporary protection must be in accordance with that regime, though Declaration No 17 on Article 73k of the 1997 TEC, *OJC* 340, 10.11.1997, p. 134, providing that ‘consultations shall be established with the United Nations High Commissioner for Refugees...on matters relating to asylum policy’ has been suppressed.

⁹² See Julia Van Dessel, *op. cit.*, p. 447 ff.

The UNHCR has been collecting the biometrics of asylum seekers since the 2000s as part of its humanitarian actions⁹³. It developed a proGrs database for verification purposes⁹⁴ and later tested a Biometric Identity Management System in Thailand⁹⁵. The latter is part of the Population Registration and Identity Management EcoSystem⁹⁶ that will be extended to additional third countries, namely: Egypt, Ethiopia, Iraq, Jordan, Kenya, Lebanon, Sudan, and Uganda⁹⁷. The UNHCR has adopted its own Guidance on data protection⁹⁸. Notwithstanding the concerns linked to the processing of biometric data performed by the agency itself⁹⁹, the Guidance states that ‘[...] UNHCR is often required to process personal data of persons of concern, including to share personal data with implementing partners and/or third parties [...] including governments, intergovernmental, non-governmental organizations, UN agencies, community-based organizations, universities, the judiciary and the private sector’¹⁰⁰.

According to the Guidance, third parties are required to adopt an equivalent or comparable level of data protection and, specifically, to adopt basic principles of personal data processing, that is: legitimate and fair processing, purpose specification, necessity and proportionality, accuracy, respect for the rights of data subjects, confidentiality, security, accountability, and

⁹³ Katja Lindskov Jacobsen, “New forms of intervention: the case of humanitarian refugee biometrics”, in Nicolas Lemay-Hébert, *Handbook on intervention and statebuilding*, Cheltenham, Edward Elgar Publishing, 2019, pp. 270-281, and Anna Lodinová, “Application of biometrics as a means of refugee registration: focusing on UNHCR’s strategy”, *Development, Environment and Foresight*, Vol. 2, No. 2, 2016, pp. 91-100.

⁹⁴ Basically, allowing undocumented migrants and refugees to access public services: Chris Burt, “UNHCR works toward self-managed refugee identity with biometrics to improve settlement outcomes”, in *BIOMETRICUPDATE.COM*, 20.09.2019, and Id., “Red Cross Norway tender seeks digital ID help for humanitarian aid”, in *BIOMETRICUPDATE.COM*, 17.07.2019; Sikhulile Dhlamini, “Technology Allows Migrant Returnees in Hargeisa to Access Services”, *News - Global*, 19.07.2019, available at www.iom.int, and Ben Perker, “Aid’s cash revolution: a numbers game”, *The New Humanitarian*, 2.11.2016, available at www.thenewhumanitarian.org. However, this practice is highly risky since it might discourage migrants from accessing basic services in case medical data are shared with the government, for example, for return purpose – see the European Council on Refugees and Exiles, “UK: NHS to Pull out of Data- Sharing Agreement with Home Office”, *ECRE Weekly Bulletin*, 16.11.2018, available at www.ecre.org.

⁹⁵ Anna Lodinová, *op. cit.*, p. 95: ‘This means that no matter where the refugees are, whether they have an identification document or not, they can be sure that they will not be lost down administrative holes or mistaken for someone else’.

⁹⁶ UNHCR, “Data of millions of refugees now securely hosted in PRIMES”, *UNHCR Blogs*, 28.01.2019, available at www.unhcr.org. PRIMES reached 7.2 biometric records in 2018 according to Chris Burt, “UNHCR reaches 7.2M biometric records but critics express concern”, *BIOMETRICUPDATE.COM*, 24.06.2019.

⁹⁷ Luana Pascu, “UNHCR to hire Interoperability Coordinator for biometric program”, *BIOMETRICUPDATE.COM*, 8.09.2019.

⁹⁸ The UNHCR, *Handbook for registration. Procedures and Standards for Registration, Population Data Management and Documentation*, Geneva, 2003.

⁹⁹ Ariel Bogle, “Biometric data is increasingly popular in aid work, but critics say it puts refugees at risk”, *ABC Science*, 21.06.2019, available at www.abc.net.

¹⁰⁰ See the UNHCR, *Guidance on the protection of personal data of persons of concern to UNHCR*, Geneva, 2018, p. 55 ff., available at www.unhcr.org.

supervision¹⁰¹. However, provided that the UNHCR periodically transfers its data to, for example, the Department of Homeland Services in the US for the purposes of resettlement¹⁰², we must point out that its Privacy Impact Assessment is not a substitute for an EU adequacy decision. Working on the interoperability aspects of its data, the UNHCR opened a call for applicants for a vacancy for an expert Interoperability Coordinator within the Identity Management and Registration Section of the Data and Identity Management Service in the UNHCR headquarters in Copenhagen in October 2019. From the call for applicants, we note that:

‘This will be a key addition to the Interoperability Program, as the role is responsible with developing guidelines from a data protection and legal/regulatory framework perspective. The Interoperability Coordinator will work with data protection, digital identity and biometrics programs of work and country operations’¹⁰³.

The IOM, for its part, has implemented a Migration Information and Data Analysis System that stores: biographical and biometric data, travel document information, entry/exit data, visa data, and vehicle/flight/vessel/data in twenty-three countries, mainly in Africa¹⁰⁴. The system has been strongly promoted by the US and it is expected to begin gathering and analysing migration data, and ‘[...] to actually put on more projects’ by suggesting potential avenues for further technical solution’¹⁰⁵. The EU is collaborating with the IOM to implement civil registers consisting of multi-purpose databases based on biometric technology. Identification systems are becoming crucial tools to promote sustainable development and to fight poverty through concerted multilateral actions¹⁰⁶. As Llaneza González highlights, the World Bank is heading another project, the Identification For Development (ID4D), together with the Bill Foundation and Melinda Gates, the United Kingdom, Australia, and the Omidyar Network¹⁰⁷. The main goals pursued by these companies consist in guaranteeing the access to services and rights by making use of digital identities in disadvantaged countries. The mission between the EU and

¹⁰¹ For this purpose, the UNHCR elaborates Privacy Impact Assessment that is internally or externally elaborated. The latter is suggested to conduct ‘DPIAs at global level that cover a set of similar processing operations. This would apply to UNHCR’s use of a number of technology products combined in the Population Registration and Identity Management Eco System (PRIMES)’, *ibid.*, p. 55.

¹⁰² The data are stored in the Automated Biometric Identification System and in the Homeland Advanced Recognition Technology System according to Chris Burt, “DHS to store tens of thousands of refugee biometric records from UNHCR”, *BIOMETRICUPDATE.COM*, 21.08.2019.

¹⁰³ *Ibidem*.

¹⁰⁴ Samuel Singler, “Biometric statehood, transnational solutionism and security devices: The performative dimensions of the IOM’s MIDAS”, *Theoretical Criminology*, Vol. 25, No. 3, 2021, pp. 454-473.

¹⁰⁵ *Ibid*, p. 465.

¹⁰⁶ The 16.9 objective of the Sustainable Development Goals available at www.un.org wants to provide legal identity for all, including birth registration, by 2030.

¹⁰⁷ Paloma Llaneza González, *op. cit.*, p. 34 ff.

the IOM¹⁰⁸ was agreed in the Joint Valletta Action Plan during the Summit of 11 and 12 November 2015¹⁰⁹ and was reaffirmed in the UN Global Compact for Migration on Safe, Orderly and Regular Migration¹¹⁰. Specifically, the EU has launched a European Union Emergency Trust Fund sealed in a constitutive agreement among the European Commission, twenty-five EU Member States, and Norway and Switzerland¹¹¹ to support ‘all aspects of stability and contribute to better migration management as well as addressing the root cause of destabilization, forced displacement and irregular migration, in particular by promoting resilience, economic and equal opportunities, security and development addressing human rights abuses’¹¹². Among others, the EU is funding¹¹³ a project to support the free movement of persons and migration in West Africa, that is implemented by a triad of partners – namely the IOM, the International Centre for Migration Policy Development, and the International Labour Organisation – under the leadership of the Economic Community of West African States (ECOWAS) Commission. The ECOWAS ID management initiative, consisting of the issuance of national biometric identity cards to be used as travel documents within the region, and replacing the ECOWAS Travel Certificate, has served as a model for developing systems in Nigeria¹¹⁴ and Mali¹¹⁵. It is not difficult to imagine that ECOWAS will follow the Union’s steps

¹⁰⁸ Resolution of the UN General Assembly No. A/RES/73/195 of 19 December 2018, *Global Compact for Safe, Orderly and Regular Migration*, and the UN General Assembly No. A/RES/73/151 of 17 December 2018, *Office of the United Nations High Commissioner for Refugees*.

¹⁰⁹ See the Valletta Summit on Migration, *Action Plan*, 11-12 November 2015, p. 8, available at www.consilium.europa.eu.

¹¹⁰ See Teresa Fajardo del Castillo, “El Pacto Mundial por una migración segura, ordenada y regular: un instrumento de soft law para una gestión de la migración que respete los derechos humanos”, *Revista electrónica de estudios internacionales*, No. 38, 2019, pp. 1697-5197, and Elspeth Guild, “The UN’s Search for a Global Compact on Safe, Orderly and Regular Migration”, *German law journal: review of developments in German, European and international jurisprudence*, Vol. 18, No. 7, 2017, pp. 1779-1795.

¹¹¹ Available at www.ec.europa.eu. Third countries represent the Sahel Region and Lake Chad area – Burkina Faso, Cameroon, Chad, Gambia, Mali, Mauritania, Niger, Nigeria, and Senegal; the Horn Africa – Djibouti, Eritrea, Ethiopia, Kenya, Somalia, South Sudan, Sudan, Tanzania, and Uganda –, and the North of Africa – Algeria, Egypt, Libya, Morocco, and Tunisia.

¹¹² ‘Enhance civil status registration (communication, practical frameworks, modernisation, exchange of information, network, training sessions) and support the creation of coherent and robust Civil Registry systems, as well as the issuance of secure identity cards and passports, in line with relevant regional initiatives’ in Article 2 of the constitutive agreement, available at www.consilium.europa.eu.

¹¹³ With the Global Gateway initiative, the EU allocated 150 billions of euros according to “Le sixième sommet entre l’Union européenne et l’Union africaine a posé les fondations d’un partenariat renforcé et pragmatique pour la prospérité des deux continents”, *Bulletin Quotidien Europe*, No. 12894, 19.2.2022.

¹¹⁴ See Chris Burt, “Nigeria moves Nigeria moves to implement to implement biometric ECOWAS card ECOWAS card with \$41M MoU with \$41M MoU”, *BIOMETRICUPDATE.COM*, 25.04.2019.

¹¹⁵ Joint Statement by the Council and the Representatives of the Governments of the Member States meeting within the Council, the European Parliament and the European Commission, *THE EUROPEAN CONSENSUS ON HUMANITARIAN AID. The humanitarian challenge*, available at www.ec.europa.eu.

in the management of information, yet it remains to be seen whether continental human and fundamental rights parameters will also be defined¹¹⁶.

In 2010, the IOM adopted its own Data Protection Manual¹¹⁷, gathering a set of core data protection principles, namely: lawfulness and fairness, purpose limitation, data quality, consent, confidentiality, access and transparency, data security, accountability, and remedies. It also sets forth (soft) rules on the transfer and retention of personal data, as well as any exceptions applicable to the above-mentioned principles. The transfer of personal data to third countries is allowed as long as it satisfies three main conditions that must be guaranteed in writing:

- first, the explicit consent of the data subject should be obtained at the time of collecting the personal data, as far as possible, but ‘difficulties of obtaining explicit consent at the time of transfer may be taken into account, if it is reasonably justified’¹¹⁸;
- second, personal data must be transferred for a specific purpose according to the principle of data minimisation, and
- third, the data controllers are expected to comply with ‘a due diligence exercise’ to assess the existence of adequate safeguards – i.e., confidentiality through encryption techniques, and the respect of the rights and interests of the data subject.

If the transfer of personal data is not laid down in a written contract, it must be performed on a case-by-case basis. However, in the case of ‘implementing partners’ – such as the UNHCR – the data controller must only verify whether the third party continues to respect the adequate standard conditions of transfer. Interestingly, the IOM Data Protection Manual makes explicit reference to law enforcement authorities and to Europol’s requests to access personal data. To execute their requests, the prior approval of the IOM Office of Legal Affairs is needed in respect of the principle of the consent of the data subject. Indeed, any exception to the principles set forth therein requires the development of a ‘risk-benefit assessment’ that must be proportionate to any benefits gained from the derogation.

¹¹⁶ A critic has been made Francesca Tassinari, 2021, “The externalisation of Europe's data protection law in Morocco: an imperative means for the management of migration flows”, *loc. cit.*

¹¹⁷ See the IOM, *IOM Data Protection Manual*, Geneva, 2010, available at www.iom.org.

¹¹⁸ *Ibid.*, p. 51.

The EU-ICRC dialogue¹¹⁹ has its roots in the Geneva Conventions of 1949, its Protocols of 1977, and the ICRC Statutes¹²⁰ Member States take part in. Humanitarian aid is a shared – or better, parallel – competence¹²¹ in which the EU is expected to cooperate with its Member States according to the European Consensus on Humanitarian Aid¹²². Although strictly connected to the EU competence on civil protection, humanitarian aid is an EU express external competence¹²³ which we have heard plenty about recently, because of the 2022 war in Ukraine¹²⁴. The European Commission Directorate General for European Civil Protection and Humanitarian Aid Operations (DG ECHO) is responsible for allocating the funds for all humanitarian purposes, in particular in the context of “forgotten crises” where new technologies, including interoperability¹²⁵, are deemed to bring unprecedented solutions¹²⁶.

¹¹⁹ On the strict relationship between the EU and the EU see the Editor’s Note, “Discussions: What are the future challenges for humanitarian action?”, *International Review of the Red Cross*, Vol. 93, No. 884, 2011, pp. 899-914, where the ex-Commissioner of the European Commission Delegation on European Civil Protection and Humanitarian Aid, Operations Kristalina Georgieva, and the President of the ICRC, Jakob Kellenberger, underlined the strict relationship existing between humanitarian aid and cooperation for development.

¹²⁰ ICRC, *Statutes of the International Committee of the Red Cross*, adopted on 21 December 2017, and entered into force on 1 January 2018, available at www.icrc.org, stating that the ICRC is an independent, neutral, and impartial actor.

¹²¹ See also Fulvio Attino, “EU’s Humanitarian and Civil Protection Aid: Italy’s Eccentric and ECHO-Consistent Policy”, *Romanian Journal of European Affairs*, Vol. 16, No. 24, 2016, pp. 24-43.

¹²² Joint Statement by the Council and the Representatives of the Governments of the Member States meeting within the Council, the European Parliament and the European Commission, *OJ C 25*, 30.1.2008, pp. 1-12. However, the founding Treaties do not make any express reference to International Humanitarian Law as noted by Myriam Benlolo-Carabot, Ulas Candas, and Eglantine Cujo, *Union Européenne et droit international: En l’honneur de Patrick Daillier*, Paris, Editions Pedone, 2012, p. 561 ff.: ‘This evolution is the result of the development of the Common Foreign and Security Policy (CFSP) and its operational arm, the European Security and Defence Policy (ESDP), but also of certain events such as the break-up of the former Yugoslavia and the Gulf War’ (our own translation).

¹²³ Article 214 TFEU.

¹²⁴ See, for example, “L’acheminement de l’aide d’urgence de l’UE à l’Ukraine et aux pays voisins monte en puissance”, *Bulletin Quotidien Europe*, No. 12911, 16.3.2022; “L’UE accroît son aide à l’Ukraine et aux pays voisins au moyen de la réserve d’équipements médicaux RescEU et de centres logistiques”, *Bulletin Quotidien Europe*, No. 12904, 5.3.2022, and “L’UE annonce plus de 500 millions d’euros d’aide pour l’Ukraine et les pays voisins et poursuit la coordination des biens acheminés”, *Bulletin Quotidien Europe*, No. 12902, 3.3.2022.

¹²⁵ Council of the EU, *Digitalisation in humanitarian aid: opportunities, challenges and recommendations*, 15048/21, Brussels, 17 December 2021, p. 18:

‘[...] Given the concerns about privacy and data protection, as well as the need for technological skills and system interoperability to effectively implement technological innovations in humanitarian assistance, shared technological standards are needed in the sector, especially in co-creation settings with non-traditional humanitarian actors [...]. This could include, for instance, requirements for both donors and implementing partners to have an “exit strategy” at the end of a project (in terms of what the produced database will become). Policy work at EU level is thus very important, and DG ECHO has a key role to play in supporting the development of common standards around the safe and responsible use of digital tools and best practices across the sector (Interviews October-November 2021). This is a responsibility that comes with being a leading humanitarian donor. The fact that the EU promotes a human-centric digital transformation is a positive sign in this regard [...].’

¹²⁶ Kristin Bergtora Sandvik, Maria Gabrielsen Jumbert, John Karlsrud and Mareile Kaufmann, “Humanitarian technology: a critical research agenda”, *International Review of the Red Cross*, Vol. 96, No. 893, 2014, pp. 219-242, and Andreia Ribeiro and Vania Baldi, *The Potential Role of Digital Technologies in the Context of Forced Displacement*, Cham, Springer International Publishing, 2018.

Lacking its own operational apparatus, DG ECHO supports other international or non-governmental organisations, such as the ICRC¹²⁷, in reacting to humanitarian crises. The ICRC is an independent, neutral, impartial, private association under Swiss law that provides humanitarian assistance in third countries and, possibly, within the EU¹²⁸. During the negotiations around the GDPR, the ICRC worried that the instrument would have breached the flow of information from the National Red Cross Society of a Member State to other National Societies of the Red Cross/Red Crescent and to ‘other humanitarian organisations in third States, including those which do not yet benefit from an adequacy decision’¹²⁹. The ICRC alleged that it might need to transfer personal data ‘without the consent of the data subject’¹³⁰ and the GDPR would have obstructed this. It is not clear to us whether the ICRC has its own central system that gathers the data held by each National Society of the Red Cross/Red Crescent. The staff of the Spanish Red Cross, for example, uses the Sistema de Información sobre Programas para Refugiados, Inmigrantes y Solicitantes de Asilo (SIRIA) provided by the Spanish Ministry of Employment and Social Security¹³¹. According to the ICRC:

‘The ICRC and the Red Cross and Red Crescent National Societies collect, manage, transfer and store personal data in the framework of a wide range of activities such as restoring and maintaining family contacts, tracing requests from enquirers looking for close relatives, sharing of lists of sought persons, transferring of documents such as passports, various types of certificates (birth, death, education, civil status, etc.); requesting information on the fate and whereabouts of persons allegedly deprived of their liberty; etc.’¹³².

¹²⁷ Updated European Union Guidelines on promoting compliance with international humanitarian law (IHL), *OJ* C 303, 15.12.2009, pp. 12-17.

¹²⁸ See Alessandra Annoni and Francesco Salerno, *La tutela internazionale della persona umana nei conflitti armati*, Cacucci Editore, Bari, 2019, p. 14 ff. In the specific case of the EU, confront Goran Bandov and Gabrijela Gosovic, *op. cit.*, p. 31:

‘Humanitarian aid funding is primarily intended for non-EU countries, but in case of exceptional crises or disasters within the EU, it is possible to finance emergency support. For example, as a result of the current refugee crisis in Europe, Council Regulation (EU) 2016/369 of 15 March 2016 on the provision of emergency support within the Union was adopted to meet the basic needs of people affected by disasters within the EU and to reduce severe economic damage in one or several member States (Funding for humanitarian aid 2017)’.

See also Petr Popisil, “European Union External and Internal Humanitarian Aid”, *European Food and Feed Law Review*, Vol. 14, No. 6, 2019, pp. 522-527, recalling that the Fund for European Aid to the Most Deprived was established to alleviate extreme cases of poverty among EU member states including child poverty, homelessness, and food deprivation.

¹²⁹ Council of the EU, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Applicability of the General Data Protection Regulation to the activities of the International Committee of the Red Cross (ICRC)*, 8837/15, Brussels, 12 May 2015, p. 3.

¹³⁰ *Ibidem*.

¹³¹ Available at www.expinterweb.mitramiss.gob.es.

¹³² See the Council of the EU, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Applicability of the General Data Protection Regulation to the activities of the International Committee of the Red Cross (ICRC)*, 7355/15, Brussels, 25 March 2015, p. 3, and the ICRC,

The ICRC Rules on Personal Data Protection¹³³ contemplate, *inter alia*, the principles of: lawfulness and fair processing; transparent processing; processing for specific purposes; processing of adequate and relevant data; data quality; retention, deletion, and archiving of personal data; right to information, access, correction, deletion of personal data, as well as the right to object to processing and the prohibition of decisions based on non-automated processing alone; accountability; data protection by design and by default; data protection impact assessment; and data security¹³⁴. The ICRC regime on the transfer of personal data requires: a lawful basis for transfer, whether it is the data subject's consent, the vital interest of the data subject, a public interest based on the ICRC's mandate, and so on; the realisation of a risk assessment; that the processing of personal data should be limited to the specific purposes of the ICRC's processing or further permissible processing; that only limited amounts of data is transferred according to that or those purpose/s; the compatibility of the transfer with the reasonable expectations of the data subject; the provision of appropriate safeguards – e.g., encryption techniques – and a record of the transfer. Now, for systematic or large-scale data transfers, Article 23 of the ICRC Rules contemplates both contractual clauses, laid down in a partnership agreement or in a MoU, or 'a dedicated Data Transfer agreement'. If no agreement is in place, the transfer is authorised if:

- the recipient accepts the requirement to only process the data for the purpose for which it was transferred in writing, and
- the staff in charge of the transfer finds that the recipient 'has implemented technical and organisational measures that will ensure adequate protection for the Personal Data that have been transferred'¹³⁵.

Notably, the possibility to transfer personal data to the ICRC staff has been formalised under recital (112) GDPR, according to which:

'Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be

Los migrantes desaparecidos y sus familiares: recomendaciones del CICR para los responsables de formular políticas, Geneva, 2017, available at www.icrc.org.

¹³³ ICRC, *Rules on Personal Data Protection*, Geneva, 2020, and Id., *Policy on the Processing of Biometric Data by the ICRC*, Geneva, 2019, available at www.icrc.org.

¹³⁴ The principle of confidentiality was of especial concerns during the GDPR negotiations according to the Council of the EU, 8837/15, Brussels, 12 May 2015, which explains the worrisome provoked by the Euronews, "Red Cross' cyber attack exposes data of 515,000 vulnerable people", *euronews*, 21.01.2020, available at www.euronews.com.

¹³⁵ ICRC, *Rules on Personal Data Protection*, Geneva, 2020, and Id., *Policy on the Processing of Biometric Data by the ICRC*, Geneva, 2019, p. 22.

necessary for an important reason of public interest or because it is in the vital interest of the data subject’.

Therefore, the transfer of personal data from the EU to the ICRC, or between the National Red Cross and Red Crescent National Societies, falls within Article 49(1)(d) GDPR, that is, the derogation clause enabling the transfer of personal data ‘for important reasons of public interest’ on an *ad hoc* basis. In our perspective, this is the sole legal basis upon which the interconnection of large-scale IT systems and interoperability components with the UNHCR, the IOM, and the ICRC’s databases can be justified. Neither have these organisations been subjected to an adequacy decision, nor are international or administrative agreements or arrangements¹³⁶ providing appropriate guarantees in place with the EU¹³⁷ as far as the transfer of personal data is concerned. Moreover, their internal soft rules on the protection of personal data – specifically, those on the transfer of personal data – diverge significantly from the GDPR, which is regarded as the “gold standard”¹³⁸. We would then complain that even if global interoperability would be designed so as to enable *ad hoc* transfers of data only, that is, because of the necessity to accomplish with ‘important reasons of public interest’ of Article 49(1)(d) GDPR, the transfer of personal data toward UNHCR, IOM, and ICRC’s risks depriving data subjects of basic safeguards protecting their fundamental right to the protection of personal data.

1.1.2. The communication of personal data by designated authorities

Member States’ designated authorities¹³⁹ are prohibited *prima facie* from transferring personal data stored in large-scale IT systems to third countries, international organisations, or

¹³⁶ However, the UNHCR, the IOM, and the ICRC have concluded arrangements with freedom, security and justice agencies as we further analyse below.

¹³⁷ The European Commission has concluded Framework Agreements with the UNHCR – i.e., Strategic Partnership Agreement Between the United Nations High Commissioner for Refugees and the European Commission (Benita Ferrero-Waldner, Commissioner for External Relations and European Neighbourhood Policy), available at www.refworld.org – the IOM – see “IOM, European Commission and European External Action Service Strengthen Partnership”, *NEWS GLOBAL*, 15.07.2012, the text is not published but some information can be retrieved at www.iom.int and at www.ec.europa.eu – and the ICRC – i.e., Framework partnership agreement with the ICRC of 2014, available at www.ec.europa.eu – that establish principles for reciprocal cooperation.

¹³⁸ Ben Hayes, “Migration and Data Protection: Doing No Harm in an Age of Mass Displacement, Mass Surveillance and Big Data”, *International Review of the Red Cross*, Vol. 99, No. 179, 2017, pp. 179-210, p. 195, recalling the Resolution of the International Conference of Data Protection and Privacy Commissioners on *Privacy and International Humanitarian Action*, Hong Kong, 26 September 2017, available at www.globalprivacyassembly.org.

¹³⁹ Article 65(2) of the ETIAS Regulation also refers to Europol, though the point (5) of the same Article does not. The regime on the transfer of personal data applicable to Europol will be analysed in due course. The same consideration is valid for Article 35(1) of the 2013 Eurodac Regulation.

private entities outside the Union according to the VIS¹⁴⁰, the EES¹⁴¹, the ETIAS¹⁴², the Eurodac¹⁴³, and: ‘The prohibition shall also apply where those data are further processed at national level or between Member States pursuant to Directive (EU) 2016/680¹⁴⁴. However, in the cases of the VIS¹⁴⁵, the EES¹⁴⁶, and the ETIAS¹⁴⁷, communication of personal data to a third country is possible when the following conditions are met:

¹⁴⁰ Article 31(4) of the revised VIS Regulation.

¹⁴¹ Article 41(5) of the EES Regulation.

¹⁴² Article 65(5) of the ETIAS Regulation.

¹⁴³ Article 53(1) of the 2013 Eurodac Regulation.

¹⁴⁴ In the case of the ETIAS, Article 65(2) broadly states:

‘Personal data accessed from the ETIAS Central System by a Member State or by Europol for the purposes referred to in Article 1(2) shall not be transferred or made available to any third country, international organisation or private party. The prohibition shall also apply if those data are further processed at national level or between Member States’. Article 35(1) of Eurodac Regulation, instead, establishes that: ‘This prohibition shall also apply if those data are further processed at national level or between Member States within the meaning of Article 2(b) of Framework Decision 2008/977/JHA’.

¹⁴⁵ Article 9(4)(a) to (ca) and Article 22a(1)(d) to (g) of the revised VIS Regulation refer to the following data: surname (family name); first name or names (given names); date of birth; sex; surname at birth (former surname(s)); place and country of birth; current nationality and nationality at birth; the type and number of the travel document or documents and the three-letter code of the issuing country of the travel document or documents; the date of expiry of the validity of the travel document or documents; the authority which issued the travel document and its date of issue; surname (family name), first name(s), date of birth, current nationality or nationalities, sex, place of birth; type and number of the travel document; the date of expiry of the validity of the travel document; the country which issued the travel document and its date of issue.

¹⁴⁶ Article 41(6) of the EES Regulation refer to: Article 16(1)(a), (b) and (c); Article 16(2)(a) and (b); Article 16(3)(a) and (b), and 17(1)(a) of the EES Regulation. Concerning visa-required third country nationals, the data contemplated under Article 16 of the EES Regulation are: surname (family name); first name or names (given names); date of birth; nationality or nationalities; sex; the type and number of the travel document or documents and the three letter code of the issuing country of the travel document or documents; the date of expiry of the validity of the travel document or documents; the date and time of the entry; the border crossing point of the entry and the authority that authorised the entry; the date and time of the exit, and the border crossing point of the exit. The data referred to under Article 17 of the EES Regulation for visa-exempt third-country nationals, instead, are only the ones established under Article 16(1)(a), (b) and (c), namely: surname (family name); first name or names (given names); date of birth; nationality or nationalities; sex; the type and number of the travel document or documents and the three letter code of the issuing country of the travel document or documents, and the date of expiry of the validity of the travel document or documents.

¹⁴⁷ Article 65(5) of the ETIAS Regulation establishes that the data from the ETIAS Central System referred to in Article 52(4) of the ETIAS Regulation that are accessed by designated authorities for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences falling under their competence may be transferred or made available by the designated authority to a third country in individual cases. According to Article 52(4) of the ETIAS Regulation:

‘Consultation of the ETIAS Central System shall, in the event of a hit with data recorded in an application file, give access to the data referred to in points (a) to (g) and (j) to (m) of Article 17(2) which are recorded in that application file as well as to data entered in that application file in respect of the issue, refusal, annulment or revocation of a travel authorisation in accordance with Articles 39 and 43. Access to the data referred to in point (i) of Article 17(2) and points (a) to (c) of Article 17(4) recorded in the application file shall only be given if consultation of that data was explicitly requested by an operating unit in a reasoned electronic or written request submitted under Article 51(1) and that request has been independently verified and approved by the central access point. Consultation of the ETIAS Central System shall not give access to the data concerning education referred to in point (h) of Article 17(2)’.

Article 17(2)(a) to (g) and (j) to (m) include: surname (family name), first name(s) (given name(s)), surname at birth; date of birth, place of birth, country of birth, sex, current nationality, first name(s) of the parents of the applicant; other names (alias(es), artistic name(s), usual name(s)), if any; other nationalities, if any; type, number and country of issue of the travel document; the date of issue and the date of expiry of the validity of the travel

- there is an exceptional case of urgency because of:
 - an imminent danger associated with a terrorist offence, or
 - an imminent danger to the life of a person and that danger is associated with a serious criminal offence;
- the transfer of data is necessary for the prevention, detection, or investigation in the territory of the Member States, or in the third country concerned, of a terrorist offence or other serious criminal offence;

document; the applicant's home address or, if not available, his or her city and country of residence; email address and, if available, phone numbers; Member State of first intended stay, and optionally, the address of first intended stay; for minors, surname and first name(s), home address, email address and, if available, phone number of the person exercising parental authority or of the applicant's legal guardian; where he or she claims the status of family member referred to in point (c) of Article 2(1): his or her status of family member, the surname, first name(s), date of birth, place of birth, country of birth, current nationality, home address, email address and, if available, phone number of the family member with whom the applicant has family ties, his or her family ties with that family member in accordance with Article 2(2) of the Directive 2004/38/EC; in the case of applications filled in by a person other than the applicant, the surname, first name(s), name of firm, organisation if applicable, email address, mailing address and phone number if available of that person; relationship to the applicant and a signed representation declaration. Article 17(2)(i) of the ETIAS Regulation contemplates current occupation (job group), where the application is subject to the manual processing in accordance with the procedure laid down in Article 26 of the ETIAS Regulation, the Member State responsible may in accordance with Article 27 request that the applicant provide additional information concerning his or her exact job title and employer or, for students, the name of their educational establishment. Article 17(4)(a) to (c) of the ETIAS Regulation refer to the following information: whether he or she has been convicted of any criminal offence listed in the Annex over the previous 10 years and in the case of terrorist offences, over the previous 20 years, and if so when and in which country; whether he or she has stayed in a specific war or conflict zone over the previous 10 years and the reasons for the stay; whether he or she has been the subject of any decision requiring him or her to leave the territory of a Member State or of any third countries listed in Annex II to Council Regulation (EC) No 539/2001 of 15 March 2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement, *OJ L* 81, 21.3.2001, pp. 1-7, or whether he or she was subject to any return decision issued over the previous 10 years. Finally, Article 17(2)(h) of the ETIAS Regulation refers to education – primary, secondary, higher or none.

- the designated authority has access to such data in accordance with the VIS¹⁴⁸, the EES¹⁴⁹, and the ETIAS Regulations¹⁵⁰;
- the transfer is carried out in accordance with the applicable conditions set out in the LED, in particular Chapter V thereof;
- a duly motivated written or electronic request from the third country has been submitted, and
- the requesting country ensures Member States that it will reciprocally communicate the information it stores in its own information systems.

Where a transfer is made pursuant to the conditions mentioned above, this must be documented and the documentation shall, on request, be made available to the national supervisory authority referred to in Article 41(1) of the LED, together with the information on: the date and time of the transfer; the receiving competent authority; the justification for the transfer, and the personal data transferred.

The regimes foreseen in the SIS, the Eurodac, and the ECRIS-TCN Regulations take on different forms. In the case of the SIS, Regulation (EU) 2018/1861 and Regulation (EU) 2018/1862 do not foresee any derogation to the general prohibition as far as Member States'

¹⁴⁸ Articles 22n and 22o of the revised VIS Regulation lay down the procedure and conditions for law enforcement purposes to access the VIS by the designated authorities. The former establishes that, as a general rule, the designated authorities must submit a reasoned electronic or written request to the Central Access Point that has to verify that the conditions of entry are met. However, in cases of 'exceptional urgency' the Central Access Point may verify *ex post* compliance with Article 22o and, if the designated authority does not, s/he must erase without delay the data accessed. The latter sets forth that consultation must be subjected to: consultation is necessary and proportionate for the purposes of the prevention, detection or investigation of a terrorist offence or other serious criminal offence; consultation is necessary and proportionate in a specific case; reasonable grounds exist to consider that consultation of VIS data will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation, and a query of the CIR was launched in accordance with Article 22 of the Regulation (EU) 2019/817 and the reply received as referred to in paragraph 2 of that Article indicates that data is stored in the VIS.

¹⁴⁹ Articles 31 and 32 of the EES Regulation establish the procedure and conditions to access the EES by designated authorities to the EES. Similarly to what we have commented on the revised VIS Regulation, the access is subjected to a reasoned electronic or written request submitted to the Central Access Points that shall verify the compliance with the conditions of entry, that is: the access for consultation is necessary for the purpose of the prevention, detection or investigation of a terrorist offences or another serious criminal offence; the access for consultation is necessary and proportionate in a specific case, and the evidence or reasonable grounds exist to consider that the consultation of the EES data will contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation. Therefore, the EES Regulation does not contemplate the query of the CIR according to Article 22 of the IO Regulations as a *conditio sine qua non* designated authorities may ask access to the data. In any case, Article 31(2) also allows for an *ex post* verification on the conditions of entry 'where there is a need to prevent an imminent danger to the life of a person associated with a terrorist offence or another serious criminal offence'.

¹⁵⁰ Articles 51 and 52 of the ETIAS Regulation establishing the procedure and conditions to access the ETIAS Central System.

authorities¹⁵¹ are concerned. For its part, the 2013 Eurodac Regulation – as it has not yet been recast – does not establish any specific rule for PJCCM so that the considerations made above regarding Article 35 are valid. Finally, Article 18 of the ECRIS-TCN Regulation does not consider Member States’ authorities, but sets forth a general prohibition applicable to Eurojust, Europol, and the EPPO¹⁵² that will be taken into account in due course. The regime foreseen for these three systems goes back to Chapter V of the LED and recalls that the transfer of data must be necessary for the prevention of a terrorist threat, and the detection, or investigation in the territory of the Member States or in the third country of a terrorist offence or other serious criminal offence according to Article 1(1) LED. Although specifying which Member States’ designated authorities have access to the data, the VIS, EES, and ETIAS do not clarify which parties receive the data and, specifically, whether these are public or private parties – as Article 35(1)(b) LED does¹⁵³. Besides, in the cases of the VIS, the EES, and the ETIAS Regulations, neither is the authorisation to communicate or make available personal data transmitted or made available by another Member State is required¹⁵⁴, nor has the onward transfer of personal data¹⁵⁵ been regulated. Now, the scenarios contemplated by these three systems as exceptional cases of urgency do not perfectly match with the clauses on derogation for specific situations set forth under Article 38 LED. According to the LED, a transfer or ‘a category of transfers’ of personal data to a third country or an international organisation may take place:

- in order to protect the vital interests of the data subject or another person;
- to safeguard legitimate interests of the data subject, where the law of the Member State transferring personal data so provides;
- for the prevention of an immediate and serious threat to the public security of a Member State or a third country;

¹⁵¹ Article 50 of Regulation (EU) 2018/1861 and Article 65 of Regulation (EU) 2018/1862. On the exceptions established for Union agencies, instead, see *infra*.

¹⁵² Article 18 of the ECRIS-TCN Regulation: ‘Neither Eurojust, Europol, the EPPO nor any central authority shall transfer or make available to a third country, an international organisation or a private party information obtained from ECRIS-TCN concerning a third-country national. This Article shall be without prejudice to Article 17(3)’. On the exceptional regime applicable to Eurojust see *infra*.

¹⁵³ According to it: ‘the personal data are transferred to a controller in a third country or international organisation that is an authority competent for the purposes referred to in Article 1(1)’.

¹⁵⁴ Article 35(1)(c) LED. However, Article 35(2) LED recalls that:

‘Member States shall provide for transfers without the prior authorisation by another Member State in accordance with point (c) of paragraph 1 to be permitted only if the transfer of the personal data is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State and the prior authorisation cannot be obtained in good time. The authority responsible for giving prior authorisation shall be informed without delay’.

¹⁵⁵ Article 35(1)(e) LED.

- in individual cases for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or of the execution of criminal penalties, or
- in an individual case, for the establishment, exercise or defence of legal claims relating to the purposes of the prevention, investigation, detection, or prosecution of criminal offences or of the execution of criminal penalties.

The fact that the VIS, EES, and ETIAS Regulations do not expressly refer to one of those cases leaves unresolved whether a situation of imminent danger associated with a terrorist offence or of imminent danger to the life of a person associated with a serious criminal offence could be considered as an appropriate safeguard for which ‘the controller has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with regard to the protection of personal data’¹⁵⁶ instead of a specific situation. It must be noted that recital (71) LED suggests that such an assessment must consider:

- the existence of any cooperation agreement concluded between Europol or Eurojust and third countries allowing the exchange of personal data;
- the confidentiality obligations, and
- the principle of specificity, ‘ensuring that the data will not be processed for other purposes than for the purposes of the transfer’.

In addition, during this type of assessment the controller must be certain that ‘the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment’¹⁵⁷. Therefore, the controller must undertake an investigation that is, if not a general review of the third party’s legal orders, at least specific as far as the case before them is concerned.

In our view, the evaluation requirement imposed by Article 37(1)(b) LED is difficult to reconcile with the ‘exceptional case of urgency’ the VIS, EES, and ETIAS Regulations refer to. If this is the case, and even though further clarity on this point would be appreciated, the possibility to communicate personal data should be based on Article 38 LED which regulates derogations for specific situations. In these terms, the ‘imminent danger associated with a terrorist offence’ clause could reflect point (c) of paragraph 1 of Article 38; while the ‘imminent danger to the life of a person and that danger is associated with a serious criminal offence’ might be related to point (a) of paragraph 1 of Article 38 concerning the protection of ‘the vital interests of the data subject or another person’. As a last resort, Article 38(1)(d) LED could gather them together by enabling the communication of personal data ‘in individual cases for

¹⁵⁶ Article 37(1)(b) LED.

¹⁵⁷ *Ibidem*.

the purposes set out in Article 1(1)', that is, for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties. All in all, the exceptional circumstances under which the communication or disclosure of data would take place make us referring, once again, to derogation clauses that lack of any commitment on the part of the foreign authority and rely on the sole scrutiny of the transferring competent authority.

1.2. Interoperability with the Interpol's databases

Recital (15) of the IO Regulations states the following:

'The Interpol database of Stolen and Lost Travel Documents (SLTD database) enables authorised entities responsible for preventing, detecting or investigating terrorist offences or other serious criminal offences in Member States, including immigration and border control authorities, to establish the validity of a travel document. ETIAS queries the SLTD database and the Interpol Travel Documents Associated with Notices database (TDAWN database) in the context of assessing whether a person applying for a travel authorisation is likely for instance to migrate irregularly or could pose a threat to security. The ESP should enable queries against the SLTD and TDAWN databases using an individual's identity data or travel document data. Where personal data are transferred from the Union to Interpol through the ESP, the provisions on international transfers in Chapter V of Regulation (EU) 2016/679 of the European Parliament and of the Council (4), or the national provisions transposing Chapter V of Directive (EU) 2016/680 of the European Parliament and of the Council (5) should apply. This should be without prejudice to the specific rules laid down in Council Common Position 2005/69/JHA (6) and Council Decision 2007/533/JHA'.

At the time of writing, Interpol counts on eighteen databases¹⁵⁸, among which is the SLTD database which stores lost, stolen, or revoked travel documents – e.g., passports, identity cards, UN laissez-passer or visa stamps, including stolen blank travel documents – to detect and prevent the use of invalid documents for migration, borders, and security purposes¹⁵⁹. There is

¹⁵⁸ E.g., the 'effective electronic system for the storage of data on missing persons or unidentified bodies in relation to international disasters and other comparable incidents' known as Disaster Victim Identification – see the Council of the EU, *Database of missing persons and unidentified bodies – draft EU statement for the Interpol General Assembly*, 11707/1/05 REV 1, Brussels, 8 September 2005, p. 2, and the Council of the EU, *Use and optimisation of Interpol instruments to identify and find missing persons*, 6980/16, Brussels, 11 March 2016, where it is reported how Interpol's notices and databases are used by its Member States to identify and find missing persons. See also the news "INTERPOL unveils new global database to identify missing persons through family DNA", *News&Events*, 1.06.2021, available at www.interpol.int.

¹⁵⁹ For which purposes, it collaborates with third countries, international organisations, and private partners as highlighted by Ayang Macdonald, "IDnow, INTERPOL pair up on fraud prevention training", *BIOMETRICUPDATE.COM*, 21.03.2022. The EU, for its part, uses the FADO and the and Public Register of Authentic Travel and Identity Documents Online (PRADO): the former is used by the Member States and it was lastly updated in 2020 – see the Regulation (EU) 2020/493 of the European Parliament and of the Council of 30 March 2020 on the False and Authentic Documents Online (FADO) system and repealing Council Joint Action 98/700/JHA, PE/97/2019/REV/1, OJL 107, 6.4.2020, pp. 1-8; the latter, instead, is public and it is available in the official webpage of the EU Council, where a glossary on the technical terms related to security features and to security documents in general is also available. You can consult PRADO at the EU Council official webpage available at www.consilium.europa.eu. The FADO and PRADO have been put at Interpol's disposal according to the Council of the EU, *Interpol discussion paper on the use of Interpol's border security data systems*, 9004/14, Brussels, 15 April 2014.

also the TDAWN database which stores colour-coded international alerts¹⁶⁰ – including Interpol’s red notices that serve the same purpose as the European Arrest Warrant¹⁶¹ – and requests for cooperation from one state to the other members¹⁶². Thus, the documents stored in the SLTD database may be associated with one or more TDAWN alerts if they concern the same person. Both systems were developed after 11-S to strengthen cooperation among the Interpol states supporting the US in its war against terrorism. From that moment on, Interpol assumed a pro-active participation in the managing of border controls¹⁶³.

1.2.1. Issues stemming from the Interpol’s red notices

The Interpol notices mechanism is made up of two stages: first of all, the personal data entered by the consulting authority is compared to the data stored in the SLTD and TDAWN databases, resulting in a list indicating potential matches and the nature of the alerts; and, second, the requesting authority launches a notification to the owner of the alert while going through the list. The automatic nature of how national authorities usually execute the mandate of a red notification for locating and arresting persons facing prosecution or who need to serve a sentence is quite problematic. For example, refugees that left their country of origin for

¹⁶⁰ There are seven types of notices – red, yellow, blue, black, green, orange, and purple – that correspond to different warnings. A red notice serves to seek the location and arrest of persons wanted for prosecution or to serve a sentence. A yellow notice stands for a request to help locate missing persons, often minors, or to help identify persons who are unable to identify themselves. A blue notice asks to collect additional information about a person’s identity, location, or activities in relation to a crime. A black notice serves to seek information on unidentified bodies. A green notice wants to provide warning about a person’s criminal activities, where the person is considered to be a possible threat to public safety. An orange notice aims to warn of an event, a person, an object, or a process representing a serious and imminent threat to public safety. A purple notice seeks or provides information on *modus operandi*, objects, devices, and concealment methods used by criminals. The notices are published by the General Secretariat at the request of a National Central Bureau and are made available to all the Interpol’s members. Notices can also be used by the United Nations, International Criminal Tribunals, and the International Criminal Court to seek persons wanted for committing crimes within their jurisdiction, notably genocide, war crimes, and crimes against humanity. The notices are described in the Interpol’s webpage at www.interpol.int.

¹⁶¹ Article 82 of the Interpol’s Rules on *the Processing of Data*, adopted by the General Assembly in 2011 and entered into force in July 2012, available at www.interpol.int, set forth: ‘Red notices are published at the request of a National Central Bureau or an international entity with powers of investigation and prosecution in criminal matters in order to seek the location of a wanted person and his/her detention, arrest or restriction of movement for the purpose of extradition, surrender, or similar lawful action’. Interpol is used as an alternative channel for states not participating in the SIS – third countries e.g., the United Kingdom since 1 January 2021 – or in the European Arrest Warrant alerts – e.g., states parties to the EEA – provided that the European Arrest Warrant is not a Schengen *acquis* measure according to the Council of the EU, *European Arrest Warrants - Transmission via Interpol*, 6898/05, Brussels, 7 March 2005.

¹⁶² Request for cooperation are informal alerts circulated by a National Central Bureau to all or some of the Interpol’s members.

¹⁶³ Historically, Interpol reinforced the cooperation of law enforcement authorities: ‘The various INTERPOL systems rapidly became of interest to the international community, illustrated by the increase of requests to INTERPOL to take measures to contribute with national and international partners in reinforcing borders’ by Fabrizio Carlo, *How can INTERPOL contribute to future border integrity?*, LL.M. dissertation in European Joint Master’s in Strategic Border Management, University of Warsaw, 2017, p. 29.

political reasons may be targeted with a red notice that, if it results in a hit, notifies the owner of the alert issued by their persecutor¹⁶⁴. Thus, the credibility of the Interpol's red notices mechanism has been seriously undermined by the bad practice of some of its members – including the US – that do not notify the owners of the red notices. While effectively turning bad practices into a general rule, including the creation of a situation where third countries may also apply the same treatment to the EU citizens, a hit/no-hit mechanism would prevent the notification of the red notice to its owner. The misuse of the red notices mechanism stems from a lack of trust among Interpol's members¹⁶⁵, who have experienced the consequences of when the red notices mechanism lies in the hands of dictatorial regimes¹⁶⁶.

Red notices have been scrutinised by the CJEU only once. In *WS v Bundesrepublik Deutschland* the Court was asked to interpret Article 54 of the Convention implementing the Schengen Agreement, Article 50 of the CFREU, Article 21(1) TFEU and the provisions of the LED. The case concerned a red notice issued by the US to a German national who had been discontinued by the public prosecutor as s/he had fulfilled certain conditions according to German law, and as a result criminal proceedings in respect of the acts at issue could not be brought before a national court in Germany as it would breach the *res iudicata* principle¹⁶⁷. Provided that the underlying red notice was not withdrawn, WS could not move outside the German territory, as outside of Germany they would still be considered as being subject of an arrest warrant. Thus, the non-erasure of the alert brought interesting questions before the CJEU: the *ne bis in idem* principle¹⁶⁸ read in light of Article 54 of the Convention implementing the Schengen Agreement and Article 50 CFREU; the right to free movement¹⁶⁹ by virtue of Article

¹⁶⁴ Lorraine Finlay, “Explainer: what is an Interpol red notice and how does it work?”, *The Conversation*, 30.01.2019, available at www.theconversation.com.

¹⁶⁵ The US, for example, is one of the Interpol's jurisdiction that do not carry out provisional arrest on the basis of a red notice, though accompanied by a relevant bilateral or multilateral treaty according to the Global Research Centre, *INTERPOL: Red Notices*, Washington, Law Library of Congress, 2010, p. 9.

¹⁶⁶ Christopher David and Nicholas Hearn, *A Practical Guide to INTERPOL and Red Notices*, Great Britain, Bloomsbury, 2018, p. 33 ff.

¹⁶⁷ C-505/1, *WS v Bundesrepublik Deutschland*, 12 May 2021, EU:C:2021:376.

¹⁶⁸ *Ibid.*, para. 73, maintaining that the procedure of paragraph 153a of the stop for which ‘the public prosecutor of a Member State discontinues, without the involvement of a court, a prosecution brought in that State once the accused has fulfilled certain obligations and, in particular, has paid a certain sum of money determined by the public prosecutor’ should be interpreted as a final decision.

¹⁶⁹ *Ibid.*, paras. 88-89, sentencing the possibility of provisionally arresting a person subject to an Interpol's red notice in case there are doubts as to whether the principle of the *ne bis in idem* applies. However, this would not be the case when:

‘By contrast, where the authorities of a Contracting State or of a Member State to which that person travels have become aware of the fact that a final judicial decision has been taken in another Contracting State or in another Member State establishing that the *ne bis in idem* principle applies with regard to the acts covered by that red notice, where appropriate after obtaining the necessary information from the competent authorities of the Contracting State or of the Member State in which it is alleged that a public prosecution in respect of the same acts has been barred, both the mutual trust which is required between Contracting States under Article 54

54 of the Convention implementing the Schengen Agreement, prohibiting the persecution of a person having been subject to a final decision; the relationship between an Interpol's red notice, the underlying EU-US Extradition Agreement¹⁷⁰, EU law¹⁷¹, as well as the consequent lawful processing of personal data appearing in the red notice in case the principle of *ne bis in idem* applies¹⁷².

As for the latter point, the CJEU was required to assess the lawfulness of Member States' authorities recording the personal data appearing in a red notice in domestic lists of wanted persons, or the lawfulness of the retaining such a record when the data had already been inserted, as well as any further processing activity, following the application of the *ne bis in idem* principle within the Schengen area. The Court noted that the LED, that is surely applicable when Member States' authorities process the personal data contained in a red notice alert, could not be applied to Interpol 'since that organisation is not a 'competent authority' within the meaning of Article 3(7) of that directive' and that in no way did the LED or other applicable rules prohibit the processing of personal data in an Interpol red notice by virtue of the *ne bis in idem* principle set forth under the Convention implementing the Schengen Agreement¹⁷³. Therefore, the Court ruled that national authorities could register or keep the record of personal data – i.e., they can further process the personal data – corresponding to the alert for the purposes of prevention, investigation, detection, or prosecution of criminal offences or of the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. However, the Court also highlighted that the individual should have been given the ability to exercise their right to erase personal data that had been registered. Regarding

of the Convention implementing the Schengen Agreement, as noted in paragraph 80 above, and the right to freedom of movement guaranteed in Article 21(1) TFEU, read in the light of Article 50 of the Charter, preclude those authorities from making a provisional arrest of that person or, as the case may be, from keeping that person in custody'.

¹⁷⁰ Agreement on extradition between the European Union and the United States of America, *OJL* 181, 19.7.2003, pp. 27-33.

¹⁷¹ C-505/1, *WS v Bundesrepublik Deutschland*, para. 99:

'It is apparent from Article 87 of those rules that the States affiliated to Interpol are required, if a person who is the subject of a red notice is located in their territory, provisionally to arrest that person only in so far as such a measure is 'permitted under national law and applicable international treaties. In the event that the provisional arrest of a person who is the subject of an Interpol red notice is incompatible with EU law, where that notice relates to acts to which the *ne bis in idem* principle applies, a State affiliated to Interpol would therefore not fail, by refraining from making such an arrest, to fulfil its obligations as a member of that organisation'.

However, in the case at stake the Court maintained that there were no proofs that the Interpol's red notice published in 2012 concerned 'the same acts as those in respect of which WS's trial had been finally disposed of, within the meaning of Article 54 of the [Convention implementing the Schengen Agreement], in Germany'. Consequently, the CJEU justified the provisional arrest of WS on the sole basis of the Interpol's red notice.

¹⁷² *Ibid.*, paras. 107-121.

¹⁷³ *Ibid.*, para. 117.

the keeping of records, the Court affirmed that ‘they must be accompanied by a note that the person in question may no longer be prosecuted in a Member State or in a Contracting State for the same acts by reason of the *ne bis in idem* principle’¹⁷⁴. Or, in other words, the data subject must be informed and granted the right to rectify personal data.

If Advocate General Bobek’s Opinion is taken into account, the Court fell short in its reasoning in *WS v Bundesrepublik Deutschland*¹⁷⁵. The Advocate General underlined that the lawfulness of any further processing of personal data must comply with the principle of necessity¹⁷⁶. He stated this not only because of the authorities’ interests in safeguarding public security, but also in the data subject’s own interest in not having to have to prove – when relevant– the application of the *ne bis in idem* principle *sine die*¹⁷⁷. He then went on to explain that:

‘[...] the continued storage of the data with the indication that the person cannot be prosecuted for those acts because of the principle *ne bis in idem* may probably be considered to be ‘necessary’, whereas a further spreading of the information to the police forces that that person is wanted on the basis of a red notice may not be so. Clearly, such an assessment can be carried out only on a case-by-case basis, in the light of all relevant circumstances’¹⁷⁸.

Even more interesting is the fact that the referring judge asked the Court whether Interpol ensured an adequate level of protection of personal data in the light of Article 36 LED. Advocate General Bobek¹⁷⁹, but not the CJEU, analysed the compatibility of Interpol’s rules on the processing of personal data before the EU data protection *acquis* and, specifically, the LED, given that Interpol should have erased the red notice if the *ne bis in idem* principle had been applied. In the Advocate General’s words:

‘[...] The referring court states that if Interpol, in a situation such as that at issue in the main proceedings, does not ensure that the personal data contained in a red notice are duly erased or corrected, because of the applicability of the principle *ne bis in idem*, doubts may arise regarding the adequacy of Interpol’s data protection rules under Directive 2016/680. That would ultimately lead to the question – in the view of the referring court – of whether Member States should refrain from cooperating with Interpol’¹⁸⁰.

In this sense, the Advocate General noted that, although the LED regulates the transfer of personal data from the EU to third countries or international organisations, the same principles

¹⁷⁴ *Ibid.*, para. 120, *in fine*.

¹⁷⁵ Opinion of Advocate General Bobek, C505/1, *WS v Bundesrepublik Deutschland*, 19 November 2020, EU:C:2020:939.

¹⁷⁶ *Ibid.*, para. 126.

¹⁷⁷ *Ibid.*, para. 121.

¹⁷⁸ *Ibid.*, para. 125.

¹⁷⁹ *Ibid.*, paras. 129-138.

¹⁸⁰ *Ibid.*, para. 132.

set forth in Chapter V of the LED are applicable to the reverse flow of data – i.e., in cases of personal data transmission from Interpol to the EU. Advocate General Bobek sustained that:

‘[...] the situation relating to the transfer of personal data from a third party to the Union is naturally different. Once those data have entered the Union’s ‘virtual space’ any processing must comply with all the relevant EU rules. In those situations, there may, accordingly, be no need for rules such as those set out in Articles 36 to 38 of Directive 2016/680. The Union also has no interest (let alone the power) in requiring third parties to process personal data which do not originate from the Union according to rules equivalent to its own’¹⁸¹.

In these terms, the Advocate General found the referral question inadmissible as it was not related to the case in question, provided that the Interpol-EU transfer of personal data is at stake, and not the EU-Interpol transfer when a red notice alert is issued. Nevertheless, it is incorrect to maintain, as Advocate General Bobek did, that Interpol’s level of protection over personal data does not ‘interest’ the EU when the latter is the recipient of the information. Indeed, although the EU cannot impose its data protection standards on a foreign jurisdiction, it should not accept personal data gathered by a third country or international organisation in breach of human rights standards. Not only may this possibility circumvent the protection it intends to give to its own citizens and residents¹⁸², but it would also infringe its commitment in promoting the respect of human rights internationally¹⁸³.

1.2.2. Consultation of the Interpol’s databases

As all EU Members States are members of Interpol – for a total of one hundred and ninety-four members – discussions around the interoperability between Interpol’s databases and the EU systems began after the elaboration of the European Information Exchange Model¹⁸⁴ when ‘Interpol presented the I-link system and in this context explained the aspect of interoperability from Interpol’s perspective, according to which there has been a shift from linking solely single countries to linking regions together [...] such as ASEANPOL, MERCOSUR and the EU’¹⁸⁵.

Interpol has adopted two integrated solutions to facilitate connectivity with other systems, using either fixed or mobile integrated network databases, known as the Fixed Interpol Network Database and the Mobile Interpol Network Database. Both can be integrated in existing computer-assisted verification systems, while the Mobile Interpol Network Database can also

¹⁸¹ *Ibid.*, para. 136.

¹⁸² Article 3(5) TEU.

¹⁸³ Article 21(2)(b) TEU.

¹⁸⁴ See Chapter I.

¹⁸⁵ Council of the EU, *Meeting with Interpol at the level of CATS Brussels, 17 December 2009*, 6386/11, Brussels, 11 February 2010.

be used in a country without an existing system. Member States had been found to not systematically check Interpol's databases at the border crossing points, as a result, in 2010 Interpol urged the EU to oblige Member States to routinely use and implement the Fixed Interpol Network Database or the Mobile Interpol Network Database at the border crossing points¹⁸⁶.

Cooperation around the exchange of information between the EU and Interpol was firstly centralised with the SIS alerts on 'objects sought for the purposes of seizure or use as evidence in criminal proceedings shall be entered in the Schengen Information System'¹⁸⁷. Among others, the alerts covered by the SIS included information on: stolen blank official documents, misappropriated or lost, and issued identity papers – passports, identity cards, driving licences – which had been stolen, misappropriated, or lost. The Common Position 2005/69/JHA required Member States to exchange 'present and future passport data with Interpol' as soon as they stored the information in a national database, or a SIS alert was created¹⁸⁸. However, the transfer of data should have been subjected to: an adequate level of protection of personal data ensured by Interpol's members; the respect of fundamental rights and liberties regarding the automatic processing of personal data, and the Member States' decision to share data only with other Interpol members that have committed to the exchange of, at least, the same data¹⁸⁹. For their part, Member States committed to impose on their competent law enforcement authorities the duty to query Interpol databases 'each time when appropriate for the performance of their task'¹⁹⁰ and, in case of a hit, the competent authorities were to act in accordance with their national law – e.g., verify, when appropriate, the correctness of the data with the country that had entered it¹⁹¹. In addition, Member States must have set up the infrastructure required to facilitate consultation as soon as possible.

With the creation of the second generation SIS, the EU laid down the basis for connecting the SIS with the Interpol databases 'subject to the conclusion of an Agreement between Interpol and the European Union'¹⁹². This agreement should have provided the Member States with access to the data stored in the Interpol SLTD and TDAWN databases through the SIS, in

¹⁸⁶ 'About 50 countries are currently using these solutions and by the end of 2009 more than 300 million checks will have been conducted through MIND/FIND allowing the identification of 25.000 criminals and the interception of 1500 stolen or lost travel documents as well as the discovery of 4000 stolen vehicles in 2009' *ibid.*, p. 3.

¹⁸⁷ Article 100(1) Convention implementing the Schengen Agreement.

¹⁸⁸ Article 3(1) of the Council Common Position 2005/69/JHA.

¹⁸⁹ Article 3(1) of the Council Common Position 2005/69/JHA.

¹⁹⁰ Article 3(4) of the Council Common Position 2005/69/JHA.

¹⁹¹ Article 3(6) of the Council Common Position 2005/69/JHA.

¹⁹² Article 55 of the Council Decision 2007/533/JHA.

accordance with the relevant SIS alerts on stolen, misappropriated, lost, and invalidated passports. The consultation of Interpol's database through the SIS was expected to augment the checking of documents, especially during border checks¹⁹³, though Interpol pushed for its databases to also be consulted before the issuing of visas¹⁹⁴. Today, both the revised VIS Regulation¹⁹⁵ and the ETIAS Regulation¹⁹⁶ include direct checks against the SLTD and TDAWN data as a first crucial exception to the general prohibition on communicating personal data with third parties subject to the provisions of Chapter V of the EUDPR – or the ECDPR in the case of the ETIAS Regulation¹⁹⁷ – and Chapter V of the GDPR, depending on whether the transfer is performed by Union agencies and systems or national authorities.

In the case of the VIS, and for the purpose of carrying out the queries referred to in point (g) of Article 9a(4) and in point (g) of Article 22b(3) of the revised VIS Regulation, these checks are directed at assessing the entry conditions of third country nationals requesting a short- or long-stay visa in light of the Schengen Borders Code and, specifically, when evaluating whether the travel document used for the application corresponds to a travel document reported lost, stolen or invalidated in the Interpol's SLTD or to a travel document recorded in a file in Interpol's TDAWN. Thus, the creation of an application file in the VIS launches a query through the ESP to compare the data referred to in Article 9(4), (5), and (6)¹⁹⁸ of the revised VIS Regulation with that stored in SLTD and TDAWN. Verification conducted on this basis

¹⁹³ SLTD and TDWAN are accessed by law enforcement authorities during first-line checks at the borders – airport, sea ports and land crossing points. The checks follow a hit/no-hit mechanism that allows them to match the identity data of the person in the Interpol databases. When a match is found, the competent authority shall ask Interpol to retrieve the relevant data so they cannot be accessed directly.

¹⁹⁴ Council of the EU, *Meeting between the Troika of the Article 36 Committee and Interpol Brussels, 16 May 2008*, 10050/08, Brussels, 29 May 2007: '[...] the Commission also promised to endeavour to have a serious examination within the Commission about how the available Interpol tools could be used to enhance EU police cooperation', p. 7.

¹⁹⁵ Article 31(1) of the VIS revised Regulation.

¹⁹⁶ Article 65(1) of the ETIAS Regulation.

¹⁹⁷ Article 65(1) of the ETIAS Regulation.

¹⁹⁸ Specifically: surname (family name); first name or names (given names); date of birth; sex; surname at birth (former surname(s)); place and country of birth; current nationality and nationality at birth; the type and number of the travel document or documents and the three-letter code of the issuing country of the travel document or documents; the date of expiry of the validity of the travel document or documents; the authority which issued the travel document and its date of issue; place and date of the application; details of the person issuing an invitation and/or liable to pay the applicant's subsistence costs during the stay, being: in the case of a natural person, the surname and first name and address of the person; in the case of a company or other organisation, the name and address of the company/other organisation, surname and first name of the contact person in that company/organisation; Member State(s) of destination and duration of the intended stay or transit; main purpose(s) of the journey; intended date of arrival in the Schengen area and intended date of departure from the Schengen area; Member State of first entry; the applicant's home address; current occupation and employer; for students: name of educational establishment; in the case of minors, surname and first name(s) of the applicant's parental authority or legal guardian; a photograph of the applicant, in accordance with Regulation (EC) No 1683/95; fingerprints of the applicant, in accordance with the relevant provisions of the Common Consular Instructions.

should indicate if there is a risk of illegal immigration, or a risk to the security of the Member States, and whether the applicant intends to leave the territory of the Member States before the expiry of the visa¹⁹⁹. In these terms, VIS's automated checks will also support visa authorities in detecting SIS refusal of entry alerts²⁰⁰.

For its part, Article 65(1) of the ETIAS Regulation foresees that the automated comparison referred to under Article 20(2)(b) and (l) of the ETIAS Regulation and carried out by the ETIAS Central System through the ESP aims at discovering hits against: the other EU large-scale IT systems; Europol's data, and Interpol's databases. Article 20(2)(b) and (l) of the ETIAS Regulation specify that such a hit would indicate whether the travel document used for the application corresponds to a travel document reported lost, stolen or invalidated in the SLTD database, and/or whether the travel document used for the application corresponds to a travel document recorded in a file in the TDAWN database.

In any case, before concluding the treaty on the interconnection to the SLTD and TDAWN databases, the Council should have sought 'the opinion of the Commission on the adequacy of the level of protection of personal data and respect of fundamental rights and liberties regarding the automatic processing of personal data by Interpol and by countries which have delegated members to Interpol'²⁰¹. However, no adequate decision regarding Interpol has been adopted so far. Interpol's rules on the processing of personal data were last updated in 2019²⁰² and they set forth the data protection standards applicable to the organisation and its states. Yet, data protection issues concerning Interpol's red notices²⁰³ still raise concerns as they are entered according to the states' domestic legal orders with questionable results from a fundamental rights and rule of law perspective²⁰⁴. Profiting from the negotiations on the amendment of the

¹⁹⁹ Article 21 of the Visa Code.

²⁰⁰ Article 2(1)(k) of the Visa Code.

²⁰¹ Article 55(2) Council Decision 2007/533/JHA.

²⁰² Interpol's Rules on *the Processing of Data*, No. III/IRPD/GA/2011, 1 April 2019, available at www.interpol.int.

²⁰³ Jacques Semmelman and Emily Spencer Munso, "Interpol Red Notices and Diffusions: Powerful — And Dangerous — Tools of Global Law Enforcement", *The Champion*, 05.2014, pp. 28-42, available at www.nacdl.org.

²⁰⁴ Council of the EU, - *"Withdrawal of Interpol arrest warrant for Mr Zakayev"*, 5810/04, Brussels, 30 January 2004, concerning the insertion of an alert by Russia on a Chechen minister, Mr Akhmed Zakayev. His extradition was denied by the United Kingdom and Denmark until he was recognised political refugees – see also the Council of the EU, *Preliminary draft reply to question for written answer e-009274/2014 - Marina Albiol Guzmán (GUE/NGL) Role of the Council in negotiating Interpol Resolution AG-2010-RES-10*, 6000/15, Brussels, 9 February 2015, concerning an Argentinean judge's request to the Spanish Government to arrest twenty former high-ranking State officials investigated for their involvement in crimes against humanity during the Franco dictatorship. Finally, the Council of the EU, *"Interpol warrant against Mr Beslagic"*, 5777/08, Brussels, 29 January 2008, concerned an Interpol warrant for three citizens of Tuzla (Bosnia and Herzegovina) with the accusation of war crimes regarding the Brcanska Malta case. Provided that the International Criminal Tribunal for the former Yugoslavia concluded that the accusations were inconsistent, the case was referred to the judicial authorities of

Europol mandate²⁰⁵, the European Parliament proposed to empower Europol to check Interpol's red notices as they could potentially be used as a form of political abuse²⁰⁶. However, Member States opposed this proposition and rather opted for enhancing their cooperation with Interpol through their National Contact Points and the Interpol National Central Offices²⁰⁷.

1.2.3. Toward a Cooperation Agreement between the European Union and Interpol

In the absence of an adequacy decision, any exchange of personal data between the EU and Interpol shall be set forth through an international/administrative instrument or, subsidiarily, through derogation clauses. According to the EDPS:

‘[i]t should be made clear in the negotiating directives that it is necessary to ensure that the envisaged agreement generally complies with the Charter, with the relevant horizontal data protection legislation (Regulation (EU) 2018/1725, Regulation (EU) 2016/679 and Directive (EU) 2016/680 and with the specific data protection requirements and safeguards in the basic acts establishing the EU agencies or IT systems’²⁰⁸.

During session No. 88 of the Interpol General Assembly, held between 5 and 18 October 2019, the General Secretariat was given the mandate to enter into negotiations with the EU for concluding a cooperation agreement ‘which may address, inter alia, the exchange of information, granting EU access to the INTERPOL Information System, and cooperation with EU agencies within the European Union and in non-EU regions’²⁰⁹. In April 2021, the Council authorised the European Commission to undertake negotiations to conclude an EU-Interpol Cooperation Agreement on the basis of Article 218(3) and (4) TFEU²¹⁰. Despite the fact that the recourse to Article 218 TFEU makes us think of an international agreement, we believe that

Bosnia and Herzegovina that released Mr Beslagic. Therefore, the relevant arrest warrant – and the relevant alert – should have been invalidated in order to enable him to leave Bosnia.

²⁰⁵ See *infra*.

²⁰⁶ See Council of the EU, *Proposition de Règlement du Parlement Européen et du Conseil modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation – Préparation du trilogue*, 5370/22, Brussels, 24 January 2022, p. 3.

²⁰⁷ *Ibidem*.

²⁰⁸ Opinion of the EDPS No. 8/2021 on the Recommendation for a Council decision authorizing the opening of negotiations for a cooperation agreement between the EU and INTERPOL, Brussels, 25.05.2021, p. 2.

²⁰⁹ The Resolution No. 5 of the session No. 88 of the Interpol General Assembly is available in the Interpol's official webpage at www.interpol.int.

²¹⁰ Recommendation for a Council Decision authorising the opening of negotiations for a cooperation agreement between the European Union and the International Criminal Police Organisation (ICPO- INTERPOL), COM(2021) 177 final, Brussels, 14.4.2021. The agreement is concluded by the EU only on the assumption that it is based on common names that would be undermined in the event of interference by Member States. Thus, the European Commission claims to have exclusive competence under the Europol Regulation, the EBCG Agency Regulation, the Eurojust Regulation, the EPPO Regulation, the IO Regulations, the ETIAS Regulation, and the Schengen Borders Code with regard to Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders, OJ L 74, 18.3.2017, pp. 1-7.

the range of the envisaged instrument needs further consideration as long as Interpol's international subjectivity remains unclear. Although Interpol's Constitution²¹¹ qualifies as a constitutive treaty under public international law, founding a separate international organisation²¹², its Article 41 does not confer treaty-making power to it but requires it to 'establish relations and collaborate with other intergovernmental or non-governmental international organizations'. The wording used in Article 41 means that we cannot give Interpol's international subjectivity for granted. Indeed, the cooperation agreements that Interpol has so far concluded with, for example, international organisations or governments and public authorities are MoUs²¹³. Should the EU-Interpol Cooperation Agreement be agreed – no matter what procedure is followed –, the parties should be clear about its range, and point out whether it has a binding/non-binding and legislative/administrative nature – i.e., who is bound by the agreement and who is responsible in cases of infringement²¹⁴. On closer inspection, this clarification must come from both sides: on the one hand, the Union must clarify whether the agreement is based on Article 218 TFEU or not; on the other hand, Interpol shall clarify whether it is accountable itself, as an international organisation, whether its member states are, or whether they are both.

The cooperation is expected to develop on multiple layers which gives the envisaged agreement a 'highly heterogeneous nature'²¹⁵:

- first, at the operational level, Europol and Interpol will be granted reciprocal direct access to their respective databases, for the moment, the information will be exchanged through Interpol's Liaison Officer at Europol or the agency's Liaison Officer at Interpol;
- second, the EU's AFSJ large-scale IT systems – especially the ETIAS and the VIS – will be made interoperable with Interpol's SLTD and TDAWN databases, without revealing the information to the owner of the Interpol alert;
- third, Europol, the EBCG Agency, Eurojust, and EPPO will be given direct access to Interpol's databases – either directly or through a hit/no-hit basis – for the performance of their tasks and in full respect of their mandates.

²¹¹ Constitution of the ICPO-INTERPOL, adopted by the General Assembly at its 25 session, Vienna, 1956, available at www.interpol.int.

²¹² See the study conducted by Rutsel Silvestre J. Martha, *The Legal Foundations of INTERPOL*, Oxford/Portland/Oregon, Hart Publishing, 2010.

²¹³ Consult the cooperation agreements available at www.interpol.int.

²¹⁴ See the reflections we made in Chapter IV.

²¹⁵ Opinion of the EDPS No. 8/2021 on *the Recommendation for a Council decision authorizing the opening of negotiations for a cooperation agreement between the EU and INTERPOL*, Brussels, 25.05.2021, p. 6.

Notably, the agreement is not indispensable, either for the entry into operation of the interoperability components, or for the running of the underlying large-scale IT systems, but it is expected to facilitate ‘systematic checks’ of Interpol’s databases. However, its conclusion is subjected to the IO Regulations’ safeguard as far as the red notices mechanism is concerned. The IO Regulations prohibit the automatic communication of red notices in cases of a hit and, consequently: ‘Any queries of the Interpol databases launched via the ESP shall be performed in such a way that no information shall be revealed to the owner of the Interpol alert’²¹⁶. In this regard, different solutions have been explored:

- if Interpol refuses to change its Rules on Processing of Data, the EU should renounce the connecting of the ESP to Interpol’s SLTD and TDWAN;
- an agreement with a limited scope concerning only the Union agencies and Interpol could have been concluded, which in any case would have required re-negotiating the Europol-Interpol agreement, or
- Interpol should have changed, amended, or reinterpreted its Rules on Processing of Data provided that the consulting authority could perform a first check against SLTD and TDWAN without notifying the owner of the alert.

In any case, a hit in Interpol’s databases should not prevent the individual from travelling to the EU, but it would form an initial alarm for the border guard authorities. The main obstacles envisaged for the implementation of a hit/no-hit mechanism derive from the fact that Interpol’s states must unanimously accept a ‘distortion’ of the red notices mechanism, which is a core feature of the organisation. All in all, interoperability represents significant advancements to the facilitation of an agreement on ‘direct reciprocal access’ to the EU infrastructure and a third party’s database/s. Nevertheless, the EDPS called on the Council to specify the modalities through which Interpol’s databases would be accessed and it firmly opposed Interpol being given any direct or indirect access to the EU databases²¹⁷.

The envisaged EU-Interpol Cooperation Agreement would be split into two texts: one underpinned by Articles 16(2), 82(1) and 87(2) in conjunction with Articles 218 TFEU²¹⁸; and another one underpinned by Articles 16(2), 77(1) and (2) in conjunction with Articles 218 TFEU²¹⁹. The agreement covering PJCCM aims at enhancing cooperation between Europol,

²¹⁶ Article 9(5) of the IO Regulations.

²¹⁷ *Ibidem*.

²¹⁸ Council of the EU, *Recommendation for a COUNCIL DECISION authorising the opening of negotiations for a cooperation agreement between the European Union and the International Criminal Police Organisation (ICPO-INTERPOL)*, 9915/21, Brussels, 18 June 2021.

²¹⁹ *Ibidem*.

Eurojust, and the EPPO²²⁰ with Interpol²²¹; the agreement falling within the “freedom area”, instead, seals cooperation between the ETIAS Central Unit and the visa authorities with Interpol for the implementation of ‘preventive checks’²²². Specifically, Europol, Eurojust and EPPO would be granted access to SLTD and TDAWN data while the two agencies would also exchange operational information with Interpol. As far as the EBCG Agency is concerned, not only would the ETIAS Central Unit be granted access to Interpol’s databases for assessing the issuing of a travel authorisation²²³, but in addition, the statutory staff of the standing corps – category 1 staff²²⁴ of the EBCG Agency in charge of performing checks on individuals at the external borders²²⁵ – would grant access to the relevant Interpol databases for the performance of their tasks. According to the European Commission’s Proposal, the querying of Interpol’s databases – especially the SLTD – by Member States and Schengen Associated Countries during border checks is supported by Articles 8(3)(a)(i)²²⁶, Article 8(3)(a)(ii)²²⁷, and Article 6(1)(e) of the Schengen Borders Code²²⁸. Nevertheless, the EDPS highlighted the need to ‘clearly specify the purpose(s) and the objectives of the cooperation between Interpol and each institution, body, office and agency concerned’ in full respect of their mandates²²⁹. Specifically, the EDPS stressed the need to differentiate PJCCM from border management in light of the different applicable data protection frameworks – i.e., the LED and GDPR; to which, we would

²²⁰ Note that only twenty-two Member States over twenty-seven participate in the EPPO according to the information published at www.ec.europa.eu.

²²¹ Ireland opts-in is available in Council of the EU, *Draft Council Decision authorising the opening of negotiations for a cooperation agreement between the European Union and the International Criminal Police Organization (ICPO-INTERPOL)*, 10261/21, Brussels, 29 June 2021.

²²² See Chapter III.

²²³ Article 12 of the ETIAS Regulation.

²²⁴ Category 1 includes statutory staff deployed as members of the teams in operational areas in accordance with Article 55 of the EBCG Agency Regulation: ‘The Agency must contribute members of its statutory staff (category 1) to the standing corps to be deployed in operational areas as members of the teams with the tasks and powers provided for in Article 82 of this Regulation. Their tasks include countering cross-border crime and terrorism’.

²²⁵ Article 8(3)(a)(i) and (ii) and Article 6(1)(e) of the Schengen Borders Code.

²²⁶ ‘On entry and exit, third-country nationals shall be subject to thorough checks, which includes verifying the identity and the nationality of the third-country national and of the authenticity and validity of the travel document for crossing the border. This involves consulting the relevant databases, in particular (but not only) Interpol’s SLTD database’.

²²⁷ ‘The above check includes verifying that the travel document is accompanied, where applicable, by the requisite visa or residence permit’.

²²⁸ ‘The entry conditions of the third-country nationals include that they are not considered to be a threat to public policy, internal security, public health or the international relations of any of the Member States, in particular where no alert has been issued in Member States’ national databases for the purposes of refusing entry on the same grounds.’.

²²⁹ Opinion of the EDPS No. 8/2021 on *the Recommendation for a Council decision authorizing the opening of negotiations for a cooperation agreement between the EU and INTERPOL*, Brussels, 25.05.2021, p. 7.

add, the different legal bases underpinning the EU competences in the AFSJ. This, at least two dichotomies should be highlighted: the freedom/security one; and the AFSJ/CFSP one.

A preliminary remark could be made, provided that any query of Interpol's databases is deemed to pursue security objectives even when it is triggered during border checks. In the specific case of the ETIAS, for example, we wonder: are automated hits against Interpol's SLTD and TDAWN data serving other purposes than that of security? Should we assume that the legal basis for the agreement in the freedom section is incorrectly based on Article 77(1) TFEU, rather than Articles 82(1) and/or 87(2) TFEU? Obviously, the EBCG Agency is complex example that will keep appearing in our research due to the coexistence of security and non-security features in the EU external borders competence. A subjective approach that addresses the authority – or the system – in charge of performing the query, that is, the one accessing the data, cannot always resolve the freedom/security dichotomy. Under this rationale, if the EBCG Agency accessed a law enforcement or criminal judicial cooperation database, the underlying legal basis should be Article 77(1) TFEU even when it pursues PJCCM objectives. Similarly, with large-scale IT systems the principle of purpose limitation makes security objectives surface in 'migration' databases, too²³⁰. We should recall that in order to assess the legal basis underpinning the envisaged Cooperation Agreement its purposes, content and, eventually, context should be balanced to see whether the freedom or the security section finally prevails.

Another criticism can be raised in light of the blurring of the line dividing the AFSJ and the CFSP, especially as far as EU external action in the security field is concerned²³¹. With regard to first/second pillars agreements, Prof. Dashwood suggests referring to "CFSP/TFEU mixity" in order to avoid speculating on the preservation of a two-pillar structure after Lisbon²³². Prof. Cremona's point of view is that this may be the case regarding the EU data protection competences based on both Article 16 TFEU and Article 39 TEU. In her words: 'An agreement on data protection with [a] third country may therefore fall in part or wholly within the CFSP, with consequences for the decision-making procedure to be followed'²³³. Recalling Advocate General Kokott's words on the EU-Tanzania Agreement:

²³⁰ See Chapter III.

²³¹ See Article 67(3) TFEU and Article 21 TEU, both speaking about some kind of security. However, we have to highlight that also the freedom section and, specifically the EU external competence on migration is increasingly associated with CFSP, which arises issues on the horizontal allocation of competences – see Paula García Andrade, 2018, *op. cit.*, p. 182 ff., referring to the EU Border Assistance Mission in Libya (EUBAM Libya) and the EU military operation in the Southern Central Mediterranean (Operation Sophia).

²³² Alan Dashwood, "Mixity in the Era of the Treaty of Lisbon", in Christophe Hillion and Panos Koutrakos, *op. cit.*, pp. 351-366, p. 354.

²³³ Marise Cremona, 2010, *op. cit.*, p. 99.

‘[...] the crucial factor is that the relevant rules in Articles 82 TFEU and 87 TFEU deal only with cooperation within the Union. This can be seen, on the one hand, from a glance at the wording of the two provisions, but, on the other, it also follows from the concept of the area of freedom, security and justice, to the creation of which they contribute. It is the Union that provides its citizens with such an area and it is the Union that constitutes that area (Article 67(1) TFEU), with the emphasis on an area without internal frontiers (Article 3(2) TEU and 67(2) TFEU). [Conversely] cooperation between the Union and Tanzania is intended solely to promote international security outside the territory of the Union [...]’²³⁴.

Apart from the internal/external security dimensions highlighted by Advocate General Kokott, Prof. Blasi Casagran proposes also considering the actors involved in order to assess whether any measure being considered belongs to the AFSJ or to the CFSP: while law enforcement authorities clearly belong to the AFSJ, Prof. Blasi Casagran highlights that diplomatic and intelligence services stem from the ex-second pillar structure²³⁵. However, although intelligence services contribute to the preservation of national security, that still constitutes an exclusive prerogative of the Member States by virtue of Article 4(2) TEU *in fine*, the CJEU had treated the activities of law enforcement authorities and intelligence services almost equally when it came to evaluating the scope of application of the DPD, and now the GDPR²³⁶. In these terms, processing activities undertaken by intelligence services evidently include elements of internal inspection and may fall within the scope of the current study.

Thus, we believe that the dichotomy of the second/third pillar is better resolved under the theory of the choice of the correct legal basis so as to determine the underlying EU policy²³⁷. As Prof. García Andrade underlines, internal and external security goals increasingly blur together ‘[...] depending our internal security on peace and security beyond our borders, including, in particular, references to the fight against organised crime in cooperation with third countries and the strengthening of non-military aspects of security through judicial and police cooperation with crisis regions’²³⁸. Notably, the European Commission has advanced the elaboration of a parallel ‘instrument’ to seal its cooperation with Interpol based on Article 220 TFEU as far as the CFSP is concerned:

‘This cooperation will be in line with Article 220(2) TFEU in terms of outlining the overall cooperation framework and setting up a framework for structured dialogue at senior and technical level, between the EU and Interpol’.

²³⁴ Opinion of Advocate General Kokott, C-263/14, *European Parliament v Council of the European Union*, EU:C:2015:729, paras. 63-66. In the literature, confront for example Mauro Gatti, “Conflict of Legal Basis and the Internal–External Security Nexus: AFSJ versus CFS”, in Eleftheria Neframi and Mauro Gatti, *Constitutional Issues of EU External Relations Law*, Baden-Baden, Nomos, 2018, pp. 89-110.

²³⁵ See Cristina Blasi Casagran, 2017, *op. cit.*, pp. 84 ff.

²³⁶ See Chapter I.

²³⁷ See Annegret Engel, 2018, *loc. cit.*

²³⁸ Paula García Andrade, 2017, *loc. cit.* (our own translation).

Hence, the security services of the European Commission, the European External Action Service, the EU Council, and the European Parliament should be given access to specific Interpol databases ‘for background security checks, inquiries and internal investigations on third-country nationals, and authorising the Commission to enter and to issue controlled notifications of lost, stolen and revoked EU laissez-passers in Interpol’s Stolen and Lost Travel Documents database’²³⁹. Referring to an ‘instrument’ and to Article 220 TFEU, the European Commission seems to exclude the negotiations of a third cooperation agreement based on Articles 37 TEU and 218(3) TFEU, while opting for an implementing decision²⁴⁰. However, it is not clear which agreement the decision is supposed to ‘implement’, and we would warn that this might not be one of the envisaged Cooperation Agreement which are underpinned by AFSJ legal bases.

We recall that the possibility to merge CFSP and AFSJ features in a single agreement – e.g., the EU-Interpol Cooperation Agreement – should not be discarded, though a great interpretative effort of the founding Treaties would be required. Specifically, Article 218(6), second paragraph TFEU states that a CFSP agreement concluded with the unanimity in the Council is applicable when the ‘agreements relate exclusively to the common foreign and security policy’²⁴¹. Otherwise, the standard procedure regarding the qualified majority in the Council and the consultation of the European Parliament is sufficient²⁴² in light of the democratisation of the law-making procedure – i.e., as much participation by the European Parliament as

²³⁹ Recommendation for a Council Decision, COM(2021) 177 final, Brussels, 14.4.2021, p. 8, and the Council of the EU, *ANNEX to the Recommendation for a Council Decision authorising the opening of negotiations for a cooperation agreement between the European Union and the International Criminal Police Organisation (ICPO-INTERPOL)*, 7377/21 ADD 1, Brussels, 14 April 2021.

²⁴⁰ Note that Article 20(2) TFEU affirms that: ‘The High Representative of the Union for Foreign Affairs and Security Policy and the Commission shall implement this Article’.

²⁴¹ Article 218(6), second paragraph, TFEU. See C-658/11, *European Parliament v Council of the European Union*, paras. 58-59:

‘Therefore, in the context of the procedure for concluding an international agreement in accordance with Article 218 TFEU, it must be held that it is the substantive legal basis of the decision concluding that agreement which determines the type of procedure applicable under paragraph 6 of that provision. In particular, where the decision concluding the agreement in question is legitimately founded exclusively on a substantive legal basis falling within the CFSP, it is the type of procedure provided for in the first part of the second subparagraph of Article 218(6) TFEU that is applicable’.

²⁴² Article 218(6)(b) TFEU.

possible²⁴³. If the AFSJ and CFSP objectives are considered to be inseparable²⁴⁴, then, the European Commission should consider the feasibility of an agreement with multiple legal bases. According to settled CJEU case-law, the ordinary legislative procedure is not compatible with a special one requiring both the unanimity of the Council and the consultation of the European Parliament²⁴⁵. This position was first formulated in the *Titanium dioxide* case²⁴⁶, and was applied to the codecision²⁴⁷ and the ordinary legislative²⁴⁸ procedures. In addition, in *European Parliament v Council of the European Union* of 19 July 2012²⁴⁹, the CJEU found that the ordinary legislative procedure foreseen by Article 75 TFEU was incompatible with the Council-qualified majority procedure of Article 215(2) TFEU where the European Parliament had to be consulted as not only did the latter require the proposal to be jointly submitted by the High Representative of the Union for Foreign Affairs and Security Policy and the European Commission, but also because it required the previous adoption of a decision in the CFSP according to Chapter 2 of Title V TEU²⁵⁰. According to the Court '[...] the differences in the

²⁴³ See the C-178/03, *Commission v European Parliament and Council*, 10 January 2006, EU:C:2006:4, para. 59:

'[...] recourse to Article 133 EC jointly with Article 175(1) EC is likewise not liable to undermine the Parliament's rights because, although the first-mentioned article does not formally provide for the participation of that institution in the adoption of a measure of the kind at issue in this case, the second article, on the other hand, expressly refers to the procedure provided for in Article 251 EC. In contrast to the situation at issue in the abovementioned *Titanium dioxide* case, the use of a combination of legal bases does not therefore in this case involve any encroachment upon the Parliament's rights since recourse to Article 175(1) EC enables that institution to adopt the measure under the co-decision procedure'.

²⁴⁴ See the CJEU in *Opinion 2/00*; C-211/01, *Commission of the European Communities v Council*, 11 September 2003, EU:C:2003:452, and C-338/01, *Commission of the European Communities v Council of the European Union*, 26 January 2005, EU:C:2004:253.

²⁴⁵ See C-300/89, *Commission of the European Communities v Council of the European Communities*, para. 17 ff., where article 130s and Article 100a of the TEEC were at stake. The former contemplated the unanimity in the Council and the consultation of the European Parliament, the latter the cooperation procedure of Article 149(2) TEEC. The CJEU stated that the legal basis on the harmonisation procedure should have prevailed. However, it shall be highlighted that the CJEU is not firm on this point: in the C-166/077, *European Parliament v Council*, 3 September 2009, EU:C:2009:499, the European Parliament alleged that the correct legal basis of the Council Regulation (EC) No 1968/2006 of 21 December 2006 concerning Community financial contributions to the International Fund for Ireland, *OJ* 2006, L 409, p. 8, should have been Article 159 and not Article 308 of the 2002 TEC – the former regulated by the codecision law-making procedure, and the latter by the special law-making procedure with unanimity in the Council. According to the Court, para. 69:

'[...] It follows from the foregoing that, as the contested regulation pursues objectives set out in Articles 2 EC and 3(1)(k) EC and in Title XVII of the EC Treaty, without that title by itself conferring on the Community the power to realise those objectives, the Community legislature ought to have had recourse to both the third paragraph of Article 159 EC and Article 308 EC [...], while complying with the legislative procedures laid down therein, that is to say, both the 'co-decision' procedure referred to in Article 251 EC and the requirement that the Council should act unanimously'.

²⁴⁶ *Ibidem*.

²⁴⁷ See C-178/03, *Commission of the European Communities v European Parliament and Council of the European Union*.

²⁴⁸ C-130/10, *European Parliament v Council of the European Union*, para. 46.

²⁴⁹ *Ibidem*.

²⁵⁰ *Ibid.*, para. 47.

procedures applicable under Articles 75 TFEU and 215(2) TFEU mean that it is not possible for the two provisions to be cumulated, one with the other, in order to serve as a twofold legal basis for a measure such as the contested regulation²⁵¹.

Therefore, we believe that any merger of the AFSJ with CFSP objectives in a sole agreement is incompatible with the founding Treaties from a procedural perspective and, also, a competence one that empowers the High Representative of the Union for Foreign Affairs and Security Policy – and not the European Commission – to submit a recommendation to the Council so as to initiate negotiations with a third party²⁵². Such a merging would be preferable for only one reason, that is, the co-presence of AFSJ and CFSP elements in a unique agreement would not exclude the CJEU jurisprudence regarding the compatibility of the whole agreement – including the CFSP contents – as far as the founding Treaties were concerned²⁵³. Yet, the CJEU may enter into evaluating the lawfulness of a CFSP agreement despite the limitations foreseen in Article 24(1) TEU and the first paragraph of Article 275 TFEU through Article 218 TFEU²⁵⁴, or Article 40 TEU²⁵⁵. Provided that an AFSJ agreement was concluded by qualified majority and the consent of the European Parliament²⁵⁶, while a CFSP agreement must be adopted by the unanimity in the Council without any requirement to ask for the consent, or even consultation of, the European Parliament, we believe that an AFSJ/CFSP agreement would not be valid unless the CJEU jurisprudence on the choice of the correct legal basis was overridden. As Prof. Eeckhout observes²⁵⁷, the only way forward²⁵⁸ in cases of procedural incompatibility consists of the adoption of two separate agreements by virtue of two Council decisions – one related to the CFSP, and another related to the AFSJ under the aegis of a cross-pillar mixity. Such a division also is preferable from a data protection perspective, provided that the long-awaited Council Decision on the protection of personal data envisaged under Article 39 TEU has not yet been adopted.

In any case, the envisaged Cooperation Agreements will specify that the Member States' relations with Interpol will not be affected in the following terms: 'The Agreement should be

²⁵¹ *Ibid.*, para. 49.

²⁵² Article 218(3) TFEU.

²⁵³ Article 275 TFEU. See also Christophe Hillion, "A Powerless Court? The European Court of Justice and the Common Foreign and Security Policy", in Marise Cremona and Anne Thies, *op. cit.*, pp. 47-72, p. 57.

²⁵⁴ See C-658/11, *European Parliament v Council of the European Union*, 24 June 2014, EU:C:2014:2025, paras. 58-59.

²⁵⁵ C-263/14, *European Parliament v Council of the European Union (Tanzania)*.

²⁵⁶ Article 218(6)(v) TFEU.

²⁵⁷ Piet Eeckhout, *op. cit.*, p. 184.

²⁵⁸ The solution is not clear-cut in the doctrine where some authors even exclude the theory of the centre of gravity from the scope of the CFSP. Urging the CJEU to clarify the meaning of Article 40 TEU is Paula García Andrade, 2017, *op. cit.*, p. 139 ff.

without prejudice to the rights and obligations of the Member States in their relations with Interpol which fall outside the scope of this Agreement'. Unfortunately, the justification brought by the European Commission regarding the EU competence exercised in concluding the agreement is misleading. By referring to Article 3(2) TFEU, the European Commission looked at the legal basis justifying the existence of an exclusive competence, but this legal basis really sets forth the nature of the EU external competence – i.e., that it is exclusive – and not that it exists²⁵⁹. The European Commission affirms that '[t]he European Union has adopted common rules based on Articles 16, 77, 79, 85, 86, 87(1), (2) and 88 of the Treaty on the Functioning of the European Union on the aspects to cover in the cooperation agreement'. The belief that the EU has the competence to act externally, and on its own, requires further justification, especially in an AFSJ governed under competences shared between the Member States and the EU. Indeed, the implementation and management of the EU's large-scale IT systems confirm the internal, shared nature of the EU (operational) competence. It is true that in the external layer, the principle of subsidiarity may also advocate for the intervention of the EU; yet major difficulties would arise in cases where the Member States pushed for the conclusion of a mixed agreement²⁶⁰.

Last but not least, the EDPS highlighted that the sensitivity of the data concerned – among which, we might note, biometrics stand out – as well as the numerous third countries involved (that have *prima facie* inadequate safeguards in place) in the agreement called on the Council to undertake an in-depth impact assessment on the proportionality of the measure and its impact on the individual's fundamental rights²⁶¹. Bearing in mind that vulnerable persons might also be affected – such as migrants and asylum seekers – the EDPS warned that '[...] it should be explicitly laid down that personal data transferred by the EU to Interpol will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment'²⁶². The EDPS also recalled that: 'The EU legal framework for data protection is indeed composed of several different legal sources among which a series of EU secondary legislation which applies to specific transfers of data, prohibiting as a rule transfers to international organisations and allowing them only as a way of derogation under strict conditions'²⁶³. The EDPS recommended that the agreement be 'binding and enforceable' according to Article 46 EUDPR

²⁵⁹ See Chapter II.

²⁶⁰ See Chapter II.

²⁶¹ Opinion of the EDPS No. 8/2021 on the Recommendation for a Council decision authorizing the opening of negotiations for a cooperation agreement between the EU and INTERPOL, Brussels, 25.05.2021, p. 6.

²⁶² *Ibid.*, p. 2.

²⁶³ *Ibid.*, p. 10.

and that it ensured enforceable and effective rights to the individual²⁶⁴. The EDPS insisted on aligning the negotiating directives to the Union agencies and the EPPO's mandates in the specific case of allowed 'onward transfers' as well. Moreover, the agreement should clarify: when and under which circumstances automated decisions concerning individuals are allowed; the need for Interpol to notify breaches to the data subject and operational details on the security measures implemented to safeguard personal data transfer activities.

2. The operational transfer of personal data from freedom, security and justice agencies to third countries and international organisations

2.1. Interoperability with the Europol's Information System

Information exchange has always been a priority in the intergovernmental fight against transborder crimes. Following the European Council meeting in Luxembourg on 28 and 29 June 1991, information exchange was inserted in the Maastricht Treaty²⁶⁵ as a tool for cooperation between law enforcement authorities to prevent and combat terrorism, unlawful drug trafficking, and other serious forms of international crime – and included elements of customs cooperation²⁶⁶. This provision was mediated by the establishment of the European Police Office²⁶⁷ and completed by a Member States' Declaration annexed to the TEU²⁶⁸. As the Europol Joint Supervisory Body outlined:

‘Although international co-operation is not a new phenomenon in the police field, the Europol Convention marks the start of a European institution that provides a platform for various forms of cooperation between police forces’²⁶⁹.

The increase in transnational crimes – which in the EU's case is also attributable to the expansion of its external frontiers that results in the establishment of borders with new countries – was accompanied by the growing need for cooperation among the Member States' police

²⁶⁴ *Ibid.*, p. 9.

²⁶⁵ See Title VI of the 1992 TEU.

²⁶⁶ See Article K.1(9) of the 1992 TEU.

²⁶⁷ See Article K.1(9) of the 1992 TEU.

²⁶⁸ See the Declaration No 32 on police cooperation, *OJ C* 191, 29.7.1992, p. 108. In this declaration, Member States compromised to envisage the adoption of practical measures in areas related to the exchange of information and experience to: support national criminal investigation and security authorities, in particular in the coordination of investigations and search operations; create new databases; carry out central analysis and assessment of information in order to take stock of the situation and identify investigative approaches; collect and analyse national prevention programmes for forwarding to Member States and for drawing up Europe-wide prevention strategies, and adopt measures relating to further training, research, forensic matters, and criminal records departments.

²⁶⁹ Council of the EU, *Activity report of the Europol Joint Supervisory Body (October 1998–October 2002)*, 13899/03, Brussels, 28 October 2003, p. 7.

forces and intelligence agencies. Thus, the European Union Agency for Law Enforcement (Europol) replaced the European Police Office under the Council Decision of 6 April 2009²⁷⁰ and went into operation in 1 January 2010. With the Lisbon Treaty, a new regulation had to be adopted under the ordinary legislative procedure as Europol was one of the few agencies whose mandate was sealed in the founding Treaties²⁷¹.

The Europol Regulation defines it as a ‘hub’ for the exchange of information²⁷², with no coercive powers, and that is in charge of ‘preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy’ and ‘related criminal offences’²⁷³. In practice, Europol channels ‘information and intelligence sharing across EU Member States’²⁷⁴. Although the institutionalisation of Europol was expected to centralise the flow of the information in the EU’s

²⁷⁰ Council Decision of 6 April 2009 establishing the European Police Office (Europol), *OJ L* 121, 15.5.2009, pp. 37-66 (hereinafter the Europol Decision), substituting the Council Act of 26 July 1995 drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention), *OJ C* 316, 27.11.1995, pp. 1-32. Its institutionalisation was promoted before the long and time-consuming period required to amend the Europol Convention by three new Protocols – namely, the Council Act of 30 November 2000 drawing up, on the basis of Article 43(1) of the Convention on the establishment of a European Police Office (Europol Convention), a Protocol amending Article 2 and the Annex to that Convention, *OJ C* 358, 13.12.2000, p. 1; Council Act of 28 November 2002 drawing up a Protocol amending the Convention on the establishment of a European Police Office (Europol Convention) and the Protocol on the privileges and immunities of Europol, the members of its organs, the deputy directors and the employees of Europol, *OJ C* 312, 16.12.2002, p. 1, and Council Act of 27 November 2003 drawing up, on the basis of Article 43 (1) of the Convention on the Establishment of a European Police Office (Europol Convention), a Protocol amending that Convention, *OJ C* 2, 06.01.2004, p. 1 – and following the example of the new-born Eurojust analysed *infra*.

²⁷¹ Even if a first reference had been already inserted in Articles 29 and 30 of the 1992 TEU. Article 88 TFEU sets forth:

‘1. Europol’s mission shall be to support and strengthen action by the Member States’ police authorities and other law enforcement services and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy. 2. The European Parliament and the Council, by means of regulations adopted in accordance with the ordinary legislative procedure, shall determine Europol’s structure, operation, field of action and tasks. These tasks may include: (a) the collection, storage, processing, analysis and exchange of information, in particular that forwarded by the authorities of the Member States or third countries or bodies; (b) the coordination, organisation and implementation of investigative and operational action carried out jointly with the Member States’ competent authorities or in the context of joint investigation teams, where appropriate in liaison with Eurojust. These regulations shall also lay down the procedures for scrutiny of Europol’s activities by the European Parliament, together with national Parliaments. 3. Any operational action by Europol must be carried out in liaison and in agreement with the authorities of the Member State or States whose territory is concerned. The application of coercive measures shall be the exclusive responsibility of the competent national authorities’.

Notably, Member States have adopted hybrid operational measures to implement the judicial and police cooperation for combating cross-border crimes, such as the joint investigation teams and the special interventions units as we analyse *infra*.

²⁷² Recital (13) of the Europol Regulation. The exchange of information with Union bodies, authorities of third countries, international organisations – especially Interpol –, and relevant private parties is depicted as an indispensable activity in order to ensure the operational effectiveness – see recitals (30) ff.

²⁷³ Article 3(2) of the Europol Regulation.

²⁷⁴ See the Note from Europol in the Council of the EU, *Proposals from Europol: Improving information and intelligence exchange in the area of counter terrorism across the EU*, 7272/15, Brussels, 16 March 2015, p. 7.

hands as an alternative to the Member States' bilateral communication channels, these bilateral channels have been limiting Europol's operational "action" in both qualitative and quantitative terms²⁷⁵. Any step towards greater cooperation has been held back by: first, the lack of a national and international apparatus that is effective at enabling the information to flow among different departments within and outside a State's borders; and second, the Member States' reluctance to disseminate "confidential information"²⁷⁶.

The past few years have witnessed the growing value of information sharing and have favoured Europol's empowerment, the mandate of which has been recently been broadened. The Proposal presented by the European Commission in December 2020 and approved by the LIBE committee on 16 March 2022²⁷⁷ mandates Europol, *inter alia*, to support Member States in the establishment of '[...] large and complex datasets, addressing the big data challenge for law enforcement authorities'²⁷⁸. For this purpose, Member States have started transferring large amounts of data to Europol, though its processing has already caused the EDPS to raise concerns²⁷⁹.

²⁷⁵ Article 3 of the Europol Regulation and Annex I thereto. Since the Europol Convention was adopted, Europol's competences have been progressively enlarged to cover more and more criminal areas such as money laundering, environmental law, and cybercrime – including the counterfeiting of euros for which Europol was designated as the Central Office for the Member States of the European Union by Council Decision 2005/511/JHA of 12 July 2005 on protecting the euro against counterfeiting, by designating Europol as the Central Office for combating euro counterfeiting, *OJ L* 185, 16.7.2005, pp. 35-36. See the Danish delegation position in the Council of the EU, *Involvement of Europol in combatting environmental crime*, 5578/99, Brussels, 1 February 1999, and the Council of the EU, *Discussion Paper from Germany/Europol Drugs Unit – Suggestions for the Improvement of the EU Situation Report on Organised Crime*, 8469/99, Brussels, 19 May 1999, and the Council of the EU, *Proposal of the incoming Spanish Presidency and Europol's initiative for the establishment of a monitoring centre on cyber crime at Europol*, 15456/01, Brussels, 18 December 2001.

²⁷⁶ See the Council of the EU, *Exchange of views on the final report on mutual evaluation "Exchange of information and intelligence between Europol and the Member States among the Member States respectively"*, 25348/07, Brussels, 20 November 2007, which justifies the lack of a common understanding in the international community on confidential information according to Russell Buchan, *Cyber Espionage and International Law*, Oxford, Hart Publishing, 2018, and Antonio Segura Serrano, "Ciberseguridad y Derecho internacional", *Revista Española de Derecho Internacional*, Vol. 69, No. 2, 2017, pp. 291-299.

²⁷⁷ "Les eurodéputés confirment un premier accord sur la réforme d'Europol", *Bulletin Quotidien Europe*, No. 12913, 18.3.2022.

²⁷⁸ Concretely, Europol would be able to conduct a "pre-analysis" of data so as to discern the categories of data that fall within the categories it is enabled to process under Annex II B – Article 18(5a). Another issue debated during the negotiations concerned the Executive Director's empowerment to ask one of the Member States to open a new investigation with no transborder character – see the Council of the EU, 5370/22, Brussels, 24 January 2022, p. 4 ff.

²⁷⁹ See the EDPS Decision on *the retention by Europol of datasets lacking Data Subject Categorisation*, Brussels, 21.12.2021, on the Europol's filtering system for which the EDPS proposed a six-month retention period to filter and to extract the personal data and a twelve-month period to comply with the EDPS Decision, and the EDPS, *Annual Report*, Brussels, 2021, p. 30 ff. and p. 83 ff., on the development of machine learning models which the EDPS authorised '[g]iven the importance of machine learning models for the performance of Europol's core tasks and the progress achieved in establishing an internal governance framework for artificial intelligence systems'.

2.1.1. The Europol Information System

The management of information has always constituted Europol's main operational activity²⁸⁰. This has been progressively enhanced through the reforms to Europol's mandate in the founding Treaties and it currently encompasses different types of operational tasks regarding the processing of information in more or less direct forms²⁸¹. In order to achieve its goals, Europol was equipped with important technological apparatus. The Europol Computer System project was launched in January 1996, and it included the implementation of²⁸²:

- an information system, which resulted in the Europol Information System (EIS) at the end of 2001²⁸³;
- an analysis system made of Analysis Work Files (AWFs) that are stored separately from the EIS, which enabled the analysis and storage of comprehensive information;
- an Index System, that stores specific information based on the analysis carried out on the AWFs, and
- a liaison network, called SIENA, which supports the exchange of information among the Member States²⁸⁴.

The EIS is accessible by Europol National Units, the Member States' liaison officers and national competent authorities²⁸⁵, the Director, the Deputy Directors, and duly empowered Europol officials for consultations²⁸⁶ as well as for the retrieval of information²⁸⁷. Member States and Europol staff have direct access and can cross-check and analyse data of a strategic

²⁸⁰ See Article 5 of the Europol Convention, Article 5 of the Europol Decision, and Article 4 of the Europol Regulation.

²⁸¹ See the Council of the EU, *Third round of Mutual Evaluations "Exchange of information and intelligence between Europol and the Member States and among the Member States respectively"*, 9501/04, Brussels, 9 June 2004, p. 16.

²⁸² Notably, the 2016 Europol Regulation has abandoned these systems-specific approach and all the existing systems are planned to be gathered in a unique central data repository for which the data are processed according to the purpose limitation principle – see the Court of Auditors, *Europol support to fight migrant smuggling: a valued partner, but insufficient use of data sources and result measurement*, Luxembourg, 2021, p. 26. In this sense, Europol will be able to carry out data mining activities in a single database, cross-check, link, and classify the information – see Daniel Drewer and Vesela Miladinova, “The BIG DATA Challenge: Impact and Opportunity of Large Quantities of Information Under the Europol Regulation”, *Computer Law & Security Review*, Vol. 33, No. 3, 2017, pp. 298-308.

²⁸³ See the Council of the EU, *Europol work programme 2002*, 8141/01, Brussels, 24 April 2001, p. 17.

²⁸⁴ See the Council of the EU, *Europol Information System*, 9669/04, Brussels, 24 May 2004.

²⁸⁵ See Article 7(5) of the Europol Regulation. Yet, the Court of Auditors, *Europol support to fight migrant smuggling: a valued partner, but insufficient use of data sources and result measurement*, Luxembourg, 2021, p. 24, highlighted that the EIS needs to be better integrated with Member States' national databases in order to enable the direct access to it by their own domestic law enforcement authorities.

²⁸⁶ Article 7(1) of the Europol Decision.

²⁸⁷ Article 9 of the Europol Decision.

or thematic nature, while operational analyses can only be accessed indirectly²⁸⁸. In addition, Member States are allowed to further process the accessed information to combat forms of crime in respect of which Europol is competent, and other forms of serious crime, as set out in the Arrest Warrant Framework Decision²⁸⁹.

The Europol Regulation has further extended indirect access – i.e., on a hit/no-hit basis – to Eurojust and OLAF too²⁹⁰. In the case of Eurojust – with whom Europol has a long tradition of cooperation in the fight against crime – the agency concluded a working arrangement to allow access and searches, and to conduct cross-checking and analysis of a strategic or thematic nature. The searches are directed at ascertaining whether the information available to Eurojust or OLAF matches with the information processed by Europol²⁹¹. In this regard, Europol has to be notified which National Members, Deputies and Assistants, and Eurojust and OLAF staff members are competent to perform such searches²⁹². Member States, Union bodies, third countries and international organisations can establish important limits to processing that Eurojust, including its College, the National Members, Deputies and Assistants, as well as Eurojust and OLAF staff members must respect²⁹³. Europol, Eurojust and OLAF may also collaborate on the spot when the former agency or a Member State finds that coordination, cooperation, or support is needed in the frame of an individual investigation²⁹⁴.

Traditionally, the EIS has been fed with the data inserted by the Member States – through their National Units and/or through the liaison officers seconded to Europol – and by Europol itself. Specifically, the latter can input the data communicated by third countries²⁹⁵, international organisations, private parties²⁹⁶, or that is gathered directly²⁹⁷. Thus, while Member States are responsible for inputting and communicating the data – which implies that

²⁸⁸ In case of a hit, the information can be shared depending on the provider's provision – see Article 20 of the Europol Regulation.

²⁸⁹ Article 20(3) of the Europol Convention.

²⁹⁰ Articles 20 and 21 of the Europol Regulation.

²⁹¹ Article 21(3) of the Europol Regulation.

²⁹² Article 21(4) of the Europol Regulation.

²⁹³ Article 21(6) of the Europol Regulation.

²⁹⁴ Article 21(5) of the Europol Regulation.

²⁹⁵ The Europol Analysis System (EAS) is an operational information system that stores data coming from Europol's partners. It can be accessed by Europol staff only and it used by operational analysts within analysis projects – see the Court of Auditors, *Europol support to fight migrant smuggling: a valued partner, but insufficient use of data sources and result measurement*, Luxembourg, 2021. Note that Articles 49 and 50 of the Proposal for a Proposal for a “Prüm II” Regulation, is supposed to implement a router to facilitate the automated access of the Member States' law enforcement access to the Europol's data received from third countries and of the Europol's staff access to the Member States' database regarding those data that had been transmitted by third countries.

²⁹⁶ See Article 17(1)(c) of the Europol Regulation. This possibility was firstly inserted by Article 5(1) of the Europol Decision.

²⁹⁷ Article 17(2) of the Europol Regulation.

they ensure the legality of the data collection, the transmission to Europol and the input of the data, its accuracy, its up-to-date nature, and verification of the storage time-limits²⁹⁸ – Europol is responsible for the data processed in the EIS, the AWFs, and in the Index Systems.

The data that is to be inserted²⁹⁹ – including dactyloscopic data and DNA according to the Europol Decision³⁰⁰ – must be related to persons who, in accordance with the national law of the Member State concerned, are suspected of having committed or having taken part in a criminal offence for which Europol is competent, or those who have been convicted for such an offence; or persons for whom there are serious grounds under national law for believing that they will commit criminal offences for which Europol is competent³⁰¹. However, when the information is extracted from unfiltered datasets, Europol also processes the personal data of people falling outside its mandate, that is, people who may have no involvement whatsoever with criminal activity. Given the lack of an express provision limiting Europol's filtering activity concerning big data³⁰², the EDPS has severely reprimanded the agency and warned that it must limit the pre-selective phase as far as possible and that, in any case, this phase should last a maximum six months³⁰³. Regrettably, Member States have turned their back on the EDPS while agreeing a privileged regime for the datasets transferred to Europol before the entry into force of the amended Regulation³⁰⁴. According to this regime³⁰⁵, the pre-screening procedure will last eighteen months, renewable to three years as a maximum³⁰⁶ regarding the data submitted before the entry into force of the amended Regulation by the Member States, EPPO, Eurojust, and third countries to Europol³⁰⁷.

²⁹⁸ Article 15(1) of the Europol Decision.

²⁹⁹ See the list of data in the Annex II, lett. A), of the Europol Regulation.

³⁰⁰ Article 12(2) of the Europol Regulation.

³⁰¹ Article 18(2)(a) of the Europol Regulation.

³⁰² Despite the economic benefits of Big Data, this technology poses crucial challenges to the self-determination of human beings as it enables the prediction of individuals' behaviour and attitude based on elaborated information. Among others, Big Data functioning lacks transparency which prevents individuals from exercising their subjective right to the protection of personal data and creates a significant imbalance between the organisations holding the data and the people concerned. See, for example, the EDPS, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, Brussels, 26.03.2014, p. 9.

³⁰³ EDPS Decision on *the retention by Europol of datasets lacking Data Subject Categorisation*, Brussels, 21.12.2021.

³⁰⁴ Council of the EU, 5370/22, Brussels, 24 January 2022, p. 4.

³⁰⁵ *Ibid.*, p. 168 ff.

³⁰⁶ "Accord interinstitutionnel sur la réforme d'Europol", *Bulletin Quotidien Europe*, No. 12881, 2.2.2022.

³⁰⁷ Council of the EU, 5370/22, Brussels, 24 January 2022, p. 4.

On this basis, Europol can establish links between different criminal offences through a cross-checking operation: this engine gives Europol a comprehensive picture of organised crime activities realised within the Schengen area³⁰⁸. According to the Council:

‘The new system in the Regulation, which was strongly supported by the Council, represents a conceptually different data processing environment reflecting, from Europol's perspective, an Integrated Data Management Concept (IDMC). This will enable Europol to identify links and connections between different investigations and to detect emerging trends and patterns in organised crime (increased operational support capacity). Duplications are avoided as information can be cross-checked (flexibility and legal certainty). From a technological point of view, the current structure of the Europol Information System is fully compatible with the implementation of the new system for data processing. Any adapting of the processing and analysis structure can be done at a later stage without further adaptation of the Regulation ("technology-neutral" legal framework). It is the Management Board which adopts guidelines further specifying the procedures for processing of information by Europol in accordance with Article 18, after having consulted the EDPS’³⁰⁹.

To this end, Europol is entitled to choose the most efficient IT structure and it is currently relying on both the EIS and the AWFs³¹⁰. Unlike the EIS, the AWFs are directed at analysing specific issues related to crime and can include data on witnesses, victims, contacts, and associates. The AWFs contain a wider variety of data³¹¹ than the EIS but can only be created under an “Opening Order”. The Europol Regulation reduced the twenty-three types of AWFs down to two: one on ‘serious and organized crime’, and another on ‘counter terrorism’. Each work file includes the ‘focal points or targeted groups’ based on the type of crime³¹². With this information Europol creates two types of studies: strategic or thematic and, operational, at the request of the European Commission³¹³.

³⁰⁸ Article 18(2)(a) limits cross-checking to two types of persons: persons who are suspected of having committed or taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence, and persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences in respect of which Europol is competent.

³⁰⁹ See the Council of the EU, *Draft Statement of the Council's Reasons, Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA – Draft Statement of the Council's reasons*, 14957/15 ADD 1, Brussels, 24 February 2016.

³¹⁰ Confront the Opinion of the EDPS on the *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA*, Brussels, 31.05.2013, p. 9 ff.

³¹¹ See Annex II, lett. B), of the Europol Regulation.

³¹² Cristina Blasi Casagran, *op. cit.*, p. 133: ‘Each focal point stores different types of data complying with the purpose limitation principle. [...] Europol analysts working in focal points tend to follow the list of categories of data that they normally need to process during an ongoing investigation. Moreover, regular audits conducted by the Europol Data Protection Officer take place to supervise the adequacy of the data processed’.

³¹³ Recital (7) of the Europol Regulation. The Annex II, point (B), of the Europol Regulation specifies the categories of personal data that can be treated during the strategic analysis and the operational ones, or for facilitating the exchange of information according to Article 18(1) points (b) and (d).

The Europol Regulation specified that the exchange of information as well as its “operational analysis” – i.e., the gathering, storage, and processing of the information – must support criminal investigations and are vital for the effectiveness of Europol’s operational tasks³¹⁴. The management of information for strategic or thematic purposes, instead, aims at ‘[...] supporting and developing a criminal policy that contributes to the efficient and effective prevention of, and the fight against, crime’ and, according to our analysis, should not be systematised as an operational task³¹⁵. This type of analysis supports the Council in setting its priorities and in issuing recommendations³¹⁶.

Europol’s operative competences are further enriched by the provisions inserted in other Union, international or national, legal instruments for which the agency can be granted ‘computerised access to data from Union, international or national information systems, it may retrieve and process information, including personal data, by such means if that is necessary for the performance of its tasks’³¹⁷. In this sense, we recall:

- the Swedish Framework³¹⁸,
- the Prüm Decision,
- the TFTP³¹⁹,
- the exchange of information and cooperation concerning terrorist offences³²⁰,
- the PNR national databases³²¹, and

³¹⁴ See Recital (30) and Article 2(1)(c) of the Europol Regulation.

³¹⁵ See Article 2(b) of the Europol Regulation.

³¹⁶ Like the Europol’s Organised Crime Threat Assessment Western Africa, Russian Organised Crime Threat Assessment, Terrorism Situation and Trend Report described in the Council of the EU, *Europol General report 2009*, 10099/10, Brussels, 31 May 2010, p. 17.

³¹⁷ Article 17(3) of the Europol Regulation.

³¹⁸ See Article 6(2) of the Swedish Framework, and the Council of the EU, *Note of the French Delegation, Status of information copied to Europol pursuant to Article 6(2) of the Framework Decision 2006/960/JHA*, 15408/08, Brussels, 10 November 2008.

³¹⁹ Europol receives the copies of the data requests from the US and it is in charge of confirming that the requests comply with Article 4 of the EU-US the TFTP Agreement – e.g., that they respect the principle of minimisation of the data transmitted. See the Council of the EU, *Note of the Commission, Explanatory note the Europol mechanism under the draft TFTP mechanism*, 130/10, Brussels, 18 June 2010, assuming that this task would have fell within Europol’s competences set forth under Article 88 TFEU and Article 4 of the Europol Decision, though it actually was a new task. See also the German delegation’s Note in Council of the EU, *Europol’s role in the framework of the EU-US TFTP Agreement I and state of play of operational and strategic agreements of Europol (specific focus: the agreement on exchange of personal data and related information that Europol has with the US) - EU information policy on the TFTP Agreement*, 626/11, Brussels, 8 February 2011.

³²⁰ Council Decision 2005/671/JHA introduced a legal requirement for Member States to ensure that information on criminal investigations in respect of terrorist offences is sent to Europol.

³²¹ See the Presidency’s Note in Council of the EU, *Proposal for a Directive of the Council and the European Parliament on the use of Passenger Name Record for the prevention, detection, investigation and prosecution of terrorist offences and serious crime - possible role for Europol*, 12142/15, Brussels, 23 September 2015. The European Parliament proposed enabling Europol to submit on a case-by-case basis electronic and duly reasoned requests to a Passenger Information Unit for the transmission of specific PNR data or the results of the processing of specific PNR data. This possibility would have granted Europol the access to a decentralised databases to cross-

- the Union's large-scale IT systems³²².

In the future, Europol is also expected to rely on the interoperability architecture as the components are expected to 'cover Europol data, but only to the extent of enabling Europol data³²³ to be queried simultaneously with those EU information systems'³²⁴. Although the wording used by the co-legislators leaves some uncertainties on whether Europol's data could "migrate" into the interoperability infrastructure, we believe that this possibility must be excluded for now as the CIR does not store it³²⁵. Therefore, it is expected that the EIS will lay outside the interoperability components and that this will be queried simultaneously with the other systems through the ESP according to Article 22 of the IO Regulations³²⁶.

According to the latest Proposal presented by the European Commission in December 2020³²⁷, that has already found support from the European Parliament³²⁸, Europol's mandate could have been further enhanced by conferring upon the agency the possibility to ask Member States to insert alerts in the SIS II for law enforcement purposes³²⁹ on the basis of information from third countries and international organisations³³⁰. Also, the processing of biometrics

match relevant information – see the Europol's Note in Council of the EU, *EUROPOL/EU PNR architecture*, 13236/15, Brussels, 22 October 2015.

³²² Europol has been granted access to the six large-scale IT systems.

³²³ Article 4(16) of the IO Regulations goes back to Article 18(2)(a), (b) and (c) of the Europol Regulation. This Article does not set down the categories of personal data to be processed, but the purposes of their processing, that are: cross-checking aimed at identifying connections or other relevant links between information related to persons who are suspected of having committed or taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence, and persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences in respect of which Europol is competent; analyses of a strategic or thematic nature, and operational analyses.

³²⁴ Recital (11) of the IO Regulations.

³²⁵ Article 18 of the IO Regulations.

³²⁶ See Chapter V.

³²⁷ Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation, COM(2020) 796 final, Brussels, 9.12.2020.

³²⁸ See "Les eurodéputés confirment un premier accord sur la réforme d'Europol", *Bulletin Quotidien Europe*, No. 12913, 18.3.2022; "Conseil de l'UE et le PE s'accordent sur le rôle d'Europol dans l'introduction de nouvelles alertes dans le Système d'information Schengen", *Bulletin Quotidien Europe*, No. 12911, 16.3.2022, and "La Présidence slovène constate des progrès sur la réforme d'Europol, mais des questions restent ouvertes sur les alertes Schengen et les droits fondamentaux", *Bulletin Quotidien Europe*, No. 12859, 23.12.2021.

³²⁹ 'In order to bridge the gap in information sharing on serious crime and terrorism, in particular on foreign terrorist fighters – where the monitoring of their movement is crucial – it is necessary to ensure that upon the proposal of Europol, Member States are able to enter an alert in the interest of the Union [...]', in the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol – Mandate for negotiations with the European Parliament*, 12800/21, Brussels, 13 October 2021, p. 3. It must be noted that the European Commission initially proposed to enable Europol to directly insert in the SIS but, apparently, the Member States' delegations opposed it.

³³⁰ Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol, COM(2020) 791 final, Brussels, 9.12.2020.

would be allowed ‘where strictly necessary and proportionate for preventing or combating crime that falls within Europol’s objectives’ notwithstanding whether they are supplemented with other personal data or not³³¹. The EDPS recommended further specification on the purposes for which these alerts can be inserted and recalled that if Europol is empowered to insert alerts on illegal immigrants, even indirectly, Regulation (EU) 2018/1861 would need further amendments³³². The political agreement reached in the trialogue on the 1 February 2021³³³ was essentially the same as the position adopted within the Council on 30 June 2021³³⁴: SIS alerts will only be entered by the Member States or, in very strict circumstances, following a request made by Europol after assessing the reliability of the source of the information and the absence of any previous SIS alert on the individual³³⁵. Member States remain free to enter the requested alerts, or another type of alert, but if they refuse to take action following an “Europol alert” this is flagged by the SIRENE Bureau. In sum, even if Europol has not been allowed to enter SIS alerts directly, this reform is an important achievement for the EU within its PJCCM policies as Member States accepted the “mixing” of their operational activity with that of the agency and, consequently, they may execute SIS II alerts originally requested by the EU, rather than another Member State³³⁶.

³³¹ Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol’s cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol’s role on research and innovation – mandate for negotiations with the European Parliament*, 10414/21, Brussels, 25 October 2021, p. 52.

³³² See the Cover Note in Council of the EU, *Formal comments of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol*, 7114/21, Brussels, 18 March 2021.

³³³ Council of the EU, 5370/22, Brussels, 24 January 2022, p. 4.

³³⁴ “Les États membres de l’UE adoptent leur mandat sur les nouvelles compétences dévolues à Europol”, *Bulletin Quotidien Europe*, No. 12752, Brussels, 1.07.2021.

³³⁵ Article 37a(3) and (4) of the Council of the EU, 12800/21, Brussels, 13 October 2021.

³³⁶ Following the path of the EBCG Agency that we analyse *infra*, Europol increasingly execute its operational mandate within the Member States’ territories according to “L’agence Europol déploie des équipes aux frontières de l’Ukraine”, *Bulletin Quotidien Europe*, No. 12924, 2.4.2022.

2.1.2. Europol's agreements

As per its mandate, Europol cooperates with third party – both public and private³³⁷ – partners in order to tackle transborder organised criminal activities³³⁸ and, specifically it exchanges information, including personal data, with these third parties³³⁹. Because of its atypical international origin, Europol was recognised international subjectivity³⁴⁰ from its very beginning³⁴¹. In this sense, the conclusion of cooperation agreements with third countries and international organisations was firstly regulated under the Europol Convention³⁴² according to which: the designation of third countries and bodies with which Europol could have concluded agreements corresponded to the unanimous decision of the Council³⁴³; the negotiation of the envisaged agreement was undertaken by the Europol Executive Director under the supervision of the Council, and its conclusion depended on the unanimous vote of the Council previous opinion of the Joint Supervisory Body³⁴⁴.

³³⁷ Also, the Europol Decision inserted provisions on the transfer of personal data between Europol and private parties – entities and bodies established under the law of a Member State or a third state, especially companies and firms, business associations, non-profit organisations, and other legal persons governed by private law – and persons. Today, the Europol Regulation (Articles 25 and 26) enables Europol to receive information from private parties, to transfer them data, and to retrieve data from the publicly available sources, like media and public data and commercial intelligence providers but was prohibited from contacting them directly.

³³⁸ Article 23 of the Europol Regulation.

³³⁹ See the Council of the EU, *Report of the Europol Joint Supervisory Board in the Council of the EU*, 13899/03, Brussels, 28 October 2003, p. 14 ff.

³⁴⁰ Article 1 of the Europol Convention. Since the Europol Convention, Europol was granted legal personality which gave it contractual capacity and enabled it to 'conclude a headquarters agreement with the Kingdom of the Netherlands and to conclude with third States and third bodies within the meaning of Article 10(4) the necessary confidentiality agreements pursuant to Article 18(6) as well as other arrangements in the framework of the rules laid down unanimously by the Council on the basis of this Convention and of Title VI of the Treaty on European Union'.

³⁴¹ Dick Heimans, "The External Relations of Europol – Political, Legal and Operational Considerations", in Bernd Martenczuk (Editor) and Servaas van Thiel, *Justice, Liberty and Security: New Challenges for EU External Relations*, Brussels, VUB Press, 2008, pp. 385-387, p. 382. See for a more nuanced view Conny Rijken, "Legal and Technical Aspects of Co-operation between Europol, Third States, and Interpol", in Vincent Kronenberger, *The European Union and the International Legal Order: Discord or Harmony?*, 2001, pp. 577-603, p. 583.

³⁴² Article 18 established that personal data should have been communicated to third states and bodies only if: this was necessary in individual cases for the purposes of preventing or combating criminal offences for which Europol is competent under Article 2 of the Europol Convention; an adequate level of data protection was ensured in that State or that body, and this was permissible under the general rules within the meaning of paragraph 2 of Article 18 of the Europol Convention. Yet, the regime on the transfer of personal data was specified in the Council Act of 3 November 1998 laying down rules concerning the receipt of information by Europol from third parties, *OJ C* 26, 30.1.1999, pp. 17-18, and in the Council Act of 12 March 1999 adopting the rules governing the transmission of personal data by Europol to third States and third bodies, *OJ C* 088, 30.03.1999, pp. 1-3, repealed by the Council Act of 28 February 2002 amending the Council Act of 12 March 1999 adopting the rules governing the transmission of personal data by Europol to third States and third bodies, *OJ C* 58, 5.3.2002, p. 12.

³⁴³ Article 3(2) of the Council Act of 12 March 1999.

³⁴⁴ Article 3 of the Council Act of 12 March 1999.

As soon as Europol was institutionalised as a Union agency, the Europol Decision's implementing rules³⁴⁵ classified cooperation agreements as operational agreements or strategic agreements: the former regulated the exchange of personal data; the latter provided for the exchange of strategic or technical information³⁴⁶. It should be noted that Europol's strategy relating to cooperation agreements pursued a specific rationale: it involved ten accession states and four candidate states – namely, Bulgaria and Romania and Croatia. Operational agreements were signed with non-EU states that had already ratified Convention 108 of the Council of Europe, with Schengen partners, and with the US, and Canada. Finally, cooperation agreements were signed with the remaining Balkan states. This strategy was revised in 2004 when the Community changed its Neighbourhood Policy following the “big enlargement”. Thus, Europol's external action was politically driven to support the EU's integrationist wave as well as the EU Council's interests³⁴⁷. Although the majority of the agreements use binding wording, it must be noted that the Europol-US operational agreement does not: The agreement foresees that the parties ‘may exchange information’, ‘may carry out forms of cooperation other than the exchange of information’, and so on.

There are eleven Europol strategic agreements³⁴⁸ and they include the following foreign partners: Brazil³⁴⁹; China³⁵⁰; Russia³⁵¹; Turkey³⁵²; the United Arab Emirates³⁵³; the United Nations Office on Drugs and Crime³⁵⁴, and the World Customs Organisation³⁵⁵. Four strategic agreements have been signed with the European Central Bank³⁵⁶, European Commission³⁵⁷, the

³⁴⁵ Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information, *OJ L* 325, 11.12.2009, pp. 6-11.

³⁴⁶ While the former type of agreements last more or less one year, the conclusion of an operational agreement may took even three years according to the Council of the EU, *Presidency's Note, Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA - Discussion paper on Europol's agreements with third countries*, 13702/13, Brussels, 17 September 2013.

³⁴⁷ Florin Coman-Kund, “Europol's international cooperation between ‘past present’ and ‘present future’: reshaping the external dimension of EU police cooperation”, *Europe and the World*, 2018, Vol. 2, No. 1, pp. 1-37.

³⁴⁸ All the agreements, both strategic and operational, are published in Europol's official website at www.europol.eu.

³⁴⁹ Europol-Brazil strategic agreement of 11 April 2017.

³⁵⁰ See the draft reply of the Council of the EU, *General Secretariat of the Council to Marco Cappato (ALDE), “Human rights and Europol-China co-operation agreement”*, 12960/06, Brussels, 18 September 2006. Europol-China strategic agreement of 19 April 2017.

³⁵¹ Europol-Russia strategic agreement of 6 November 2003.

³⁵² Europol-Turkey strategic agreement of 18 May 2004.

³⁵³ Europol-United Arab Emirates strategic agreement of 7 September 2016.

³⁵⁴ Europol-United Nations Office on Drugs and Crime strategic agreement of 16 March 2004.

³⁵⁵ Europol-World Customs Organization strategic agreement of 23 September 2002.

³⁵⁶ Europol-European Central Bank strategic agreement of 2 December 2014.

³⁵⁷ Europol-European Commission strategic agreement of 18 February 2003.

European Centre for Disease Prevention and Control³⁵⁸, CEPOL³⁵⁹, the ENISA³⁶⁰, and the European Union Intellectual Property Office³⁶¹. Strategic agreements have limited value with respect to the operational flow of personal data, but they represent an interesting track to follow EU external policy regarding police cooperation³⁶². Operational agreements³⁶³, instead, regulate the exchange of personal data and have been concluded with seventeen third party countries – Albania³⁶⁴, Australia³⁶⁵, Bosnia and Herzegovina³⁶⁶, Canada³⁶⁷, Colombia³⁶⁸, Georgia³⁶⁹, Iceland³⁷⁰, Liechtenstein³⁷¹, Moldova³⁷², Monaco³⁷³, Montenegro³⁷⁴, North Macedonia³⁷⁵, Norway³⁷⁶, Serbia³⁷⁷, Switzerland³⁷⁸, Ukraine³⁷⁹, and the US³⁸⁰ –, two EU bodies

³⁵⁸ Europol-European Centre for Disease Prevention and Control strategic agreement of 25 October 2011.

³⁵⁹ Europol-CEPOL strategic agreement of 19 October 2007.

³⁶⁰ Europol-ENISA strategic agreement of 26 June 2014.

³⁶¹ Europol- European Union Intellectual Property Office strategic agreement of 4 November 2013.

³⁶² See the Council of the EU, *Presidency Note, Europol and External Relations*, 7153/04, Brussels, 8 March 2004, p. 2: ‘They facilitate the exchange of information of a general nature such as threat assessments, modus operandi, routes used, prevention strategies and can provide, as with the USA, a useful first step towards a full operational agreement’.

³⁶³ All the agreements are available in the official webpage of Europol.

³⁶⁴ Europol-Albania operational agreement of 9 December 2013.

³⁶⁵ Europol-Australia operational agreement of 20 February 2007.

³⁶⁶ Europol-Bosnia and Herzegovina operational agreement of 31 August 2016. This agreement substituted the strategic one concluded between the same parties on the 26 January 2007 – confront Article 27 of the latest operational agreement.

³⁶⁷ Europol-Canada operational agreement, the date is not specified.

³⁶⁸ Europol-Colombia operational agreement (the date is not specified). The agreement substituted the strategic agreement concluded on the 9 February 2004 – see Article 22 of the latest operational agreement.

³⁶⁹ Europol-Georgia operational agreement of 4 April 2017.

³⁷⁰ Europol-Iceland operational agreement of 28 June 2001.

³⁷¹ Europol-Liechtenstein operational agreement of 7 June 2013.

³⁷² Europol-Moldova operational agreement of 18 December 2014.

³⁷³ Europol-Monaco operational agreement of 6 October 2011.

³⁷⁴ Europol-Montenegro operational agreement of 29 September 2014.

³⁷⁵ Europol-North Macedonia operational agreement (the date is not specified). The operational agreement replaced the previous strategic one concluded on 16 January 2007 – see Article 22 of the Europol-North Macedonia operational agreement.

³⁷⁶ Europol-Norway operational agreement of 28 June 2001.

³⁷⁷ Europol-Republic of Serbia operational agreement of 16 January 2014.

³⁷⁸ Europol-Swiss Confederation operational agreement (the date is not specified). Notably, the agreement does not foresee a specific provision on the transmission of personal data but only general ones on the exchange of information.

³⁷⁹ Europol-Ukraine operational agreement of 14 December 2016. The agreement supplied the Strategic one concluded among the same parties on 4 December 2009.

³⁸⁰ In the case of the US, the Europol-US operational agreement of 6 December 2001 was sealed in the aftermath of the 11-S and had been kept under constant monitoring by the Joint Supervisory Body. It was followed by a supplemental agreement on 20 December 2002 precisely to enable the exchange of personal data. From the exchange of letters between the US and Europol it is understandable that the information to be exchanged should have covered, *inter alia*, ‘information pertaining to immigration investigations and proceedings, and to those relating to in rem or in personal seizure or restraint and confiscation of assets that finance terrorism or form the instrumentalities or proceeds of crime, even where such seizure, restraint or confiscation is not based on a criminal conviction’. See the Council of the EU, *Presidency Note, Exchange of letters related to the Supplemental*

– Eurojust³⁸¹ and the EBCG Agency³⁸² –, and one international organisation – namely, Interpol³⁸³, despite the opposition of the Europol Joint Supervisory Body³⁸⁴. Recently, another operational agreement was concluded with Denmark due to its exit from Europol³⁸⁵. Although the operational agreements follow a common thread, each of them introduces nuances that put more emphasis on some norms over others, which makes a comprehensive analysis challenging³⁸⁶.

a) The transfer of personal data through the Europol's cooperation operational agreements

After a list of definitions that, remarkably, includes personal and non-personal data within the concept of 'information', Europol's operational agreements foresee norms on: the scope of cooperation; the mode of cooperation; the exchange of information; other forms of cooperation; the principles of security and confidentiality in the terms negotiated by a separated MoU or in

Agreement between the United States of America and Europol on the exchange of personal data and related information -Opinion of the Europol Joint Supervisory Body, 1396/1/02 REV1, Brussels, 28 November 2002, p. 3. Yet, a more simply reason could have been found in that: '[...] there is no desire on the side of the USA to replace the bilateral enforcement relationship with the EU MS but it is the interest to build upon that collaboration'.

³⁸¹ See the Council of the EU, *Eurojust-Europol Note, Annual Report to the Council on co-operation between Eurojust and Europol for 2005 and 2006 (Point 2.3 of The Hague Programme)*, 17069/06, Brussels, 21 December 2006, p. 5:

'Constraints on operational co-operation arise from Europol's strict legal framework and the lack of awareness of Member States that they have to take pro-active steps to facilitate Eurojust's involvement in analysis files. Co-operation could be improved by promoting better awareness of Europol and Eurojust's respective legal frameworks, exchange of information at an earlier stage, a more systematic involvement of Eurojust in analysis files and a rapid adoption of the table of equivalence between the respective security regimes'.

The Europol-Eurojust operational agreement entered into force on the 1 January 2010 and replaced a previous one concluded in 2004.

³⁸² Since 2007, Europol and the EBCG Agency have been cooperating in the fight against illegal immigration. They elaborated a joint assessment on the high-risk routes for illegal immigration in the Western Balkan countries and, under the Mediterranean Transit Migration – a joint project run in collaboration with UNHCR – produced a Mediterranean Transit Migration working document on the joint management of mixed migration flows, in partnership with the International Centre for Migration Policy Development. See the Council of the EU, *Presidency's Note, Conclusions from the Expert Meeting on the Follow-up of the Joint Frontex Europol Report on the High Risk Routes of Illegal Migration in the Western Balkan Countries within the Frontex Risk Analysis Network*, 5685/08, Brussels, 15 February 2008. The Europol-EBCG Agency operational agreement was signed on 4 December 2015.

³⁸³ Europol-Interpol operational agreement of 5 November 2001.

³⁸⁴ See the Council of the EU, *Joint Supervisory Board's opinion in Council Decision of xx.xx.2001 authorising the Director of Europol to conclude a co-operation agreement between Europol and Interpol*, 8803/01 ADD 2, Brussels, 15 May 2001.

³⁸⁵ See the Council of the EU, *Cover Note, Addition of Denmark to the list of third States with which Europol shall conclude an agreement*, 15759/16, Brussels, 21 December 2016, and Henrik Larsen, "What the Danish 'no' vote on Justice and Home Affairs means for Denmark and the EU", *LSE European Politics and Policy (EUROPP) Blog*, 10 December 2015, available at www.wprints.lse.ac.uk.

³⁸⁶ For a critique on the meagre safeguards provided by Europol's operational agreements with regard to the legal framework set forth in the Europol Regulation, see Florin Coman-Kund, 2018, *op. cit.*, p. 199: 'Europol's international data exchanges practice so far raises thus questions regarding the observance and rigorous application of fundamental rights and data protection standards as devised by the CJEU in its case law'.

an attached Annex³⁸⁷; disputes and liability, and the terms of the agreement. Operational agreements concern Europol's fields of competences for which purpose the operational agreement may refer to: the annex attached to the Europol Decision – and the 'related criminal offences', that is, those offences committed in the commission of a crime, or that ensure the criminal's impunity; a specific list attached or included in the operational agreement. The main form of cooperation that had been agreed was the exchange of information, but it could also include:

- the exchange of specialist knowledge;
- general situation reports;
- results of strategic analysis;
- information regarding the procedure of criminal investigations;
- information on crime prevention methods;
- participation in training activities, and
- the provision of advice and support in individual criminal investigations³⁸⁸.

Europol's operational agreements do not usually prejudice other relevant treaties in place between the third country and the Member States on the exchange of information, such as Mutual Legal Assistance treaties, other co-operation agreements or arrangements, and working enforcement relationships. In the case of the Europol-Canada operational agreement, the parties expressly agreed on the possibility to refuse, postpone, or condition a request of co-operation under specific circumstances provided that the refusal could be justified.

In order to exchange the information, the third country must designate a National Contact Point so that the exchange of information with Europol is centralised; only in some operational agreements may Europol directly contact competent authorities – namely, those authorities responsible for preventing and combating criminal offences, as is stated in the Europol-Albania operational agreement – if this is considered appropriate. The National Contact Point is responsible for the review, correction and/or deletion of personal data, and may work as mediators between Europol and the private parties established, or residing in, the third country in order to enable the exchange of information with the latter. Besides, while competent authorities regularly meet and discuss issues related to the operational agreement or 'co-

³⁸⁷ See, for example, the operational agreements concluded with Albania and Australia respectively.

³⁸⁸ Other forms of cooperation agreed include: the possibility to invite third countries' experts, Europol's analysis groups that may be formalized in an association agreement according to Article 14(8) of the Europol Decision, and the reciprocal facilitation of setting up and operation of Joint Investigation Teams. Besides, from the wording of the operational agreements it is clear that while the third country is required to have a second liaison officer(s) at Europol, Europol may 'at its own discretion', decide to second its own liaison officer(s) in the third country.

operation’ in general, at a high level, and also when concerning specific areas of criminality, the National Contact Point consults Europol on policy issues and matters of common interest and may be invited to attend the meetings of the Heads of Europol National Units. The exchange of information is regulated by the provisions of the operational agreement and of the law of each party respectively. This is supposed to be realised through a secure communication line – i.e., SIENA³⁸⁹ – agreed in a separate MoU the establishment of which places burdens upon Europol while its operation is funded by both contracting parties, e.g., in the Europol-Bosnia Herzegovina operational agreement. In case of personal data transmission, the agreement clarifies that it ‘must be necessary in individual cases’ for the purposes of preventing or combating the criminal offences for which Europol is competent. Further processing activities for different purposes must be authorised by the other party, though it is not clarified whether the “different purpose” must be compatible with the initial purpose, or not. Also, operational agreements state that the parties must supply information if it was collected, stored, and transmitted in violation of human rights. However, no monitoring mechanism is in place to assess compliance with these standards. Besides, the agreements do not specify which human rights have to be respected, but go back to Article 20(4) of the Europol Decision. In some operational agreements³⁹⁰ we can also find a clause on onward transfer that authorises the transmission of data to other competent authorities; Europol, for its part, may transmit the information to the Member States’ authorities for the purpose of preventing and combating criminal offences. ‘Any other onward transfer’ must be submitted to the consensus of the other party. Indeed, the transmission of personal data is subjected to the specification of the purpose for which the data is being transmitted as well as the existence of any restrictions on its use, deletion, or destruction.

The time-limit for processing the transmitted data is related to the time needed to achieve the goal for which the data was disclosed and, in any case, it must be revised each three years. The transmission of special categories of data, such as that revealing an individual’s racial or ethnic origin, political opinions or religious or philosophical beliefs, or trade union membership and data concerning a person’s health or sexual life can be transmitted only in cases of necessity.

³⁸⁹ SIENA substituted the Information Exchange System (InfoEx) in 2007 and it is used for the exchange of information among the various actors involved, namely, Europol, Member States, and third countries that have cooperation agreements in place with Europol. Its usefulness is confirmed by the fact that SIENA was used by law enforcement authorities also outside the Europol framework – see the Court of Auditors, *Europol support to fight migrant smuggling: a valued partner, but insufficient use of data sources and result measurement*, Luxembourg, 2021, and the Second Opinion of the EDPS No. 5/2015 on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, Brussels, 24.09.2015, p. 13.

³⁹⁰ See, e.g., the Europol-Bosnia Herzegovina, and Colombia operational agreements.

Only the Europol-US supplement agreement enables it where it is ‘particularly relevance’. Finally, all communications of personal data must be recorded together with the context that legitimised its disclosure. In case the transmitted data is later considered to be incorrect, inaccurate, outdated or that it should not have been transmitted, then, the other party must be informed so as to correct or delete the data. The right to access, check, correct, and delete personal data is regulated by the third country’s law and the Europol rules. Yet, the Europol-US supplement agreement leaves clear that it ‘[...] shall not give rise to a right on the part of any private person to obtain, suppress, or exclude any evidence, or to impede the execution of a request, nor shall it derogate from any pre-existing right or a private party to do so’³⁹¹. Europol is also granted the prerogative of keeping the data received from the third country in case it needs to process it further. To enhance trust regarding the reliability of the information, the parties must eventually indicate the source of the transmitted data in accordance with the terms agreed in a separate MoU. In addition, operational agreements can insert norms regarding the security, integrity, and confidentiality of the data.

The provisions on liability allocate the responsibility of any damages caused to an individual for legal or factual errors in the exchanged information ‘in accordance with their respective legal framework’. Nevertheless, such a responsibility is limited to the satisfaction of the right to compensation of the individual while punitive or non-compensatory damages are excluded. Some agreements do not designate a specific dispute settlement mechanism³⁹², leaving the resolution of any conflict of application or interpretation of the agreement to consultation and negotiation. Others, instead, provide for the designation of three arbitrators that can issue a final binding decision³⁹³. In case of “serious failings” to comply with an agreement, they may suspend the application of the agreement temporarily, an act which does not free them from complying with their mutual obligations. Would the parties decide to terminate the operational agreement, they should agree to new terms on the use and storage of data that has already been transmitted, or they may ask for its destruction or return.

The Europol-Interpol instrument can be considered as an example of an operational agreement concluded with an international organisation, aiming at establishing and maintaining co-operation between the parties in combating forms of organised international crime according

³⁹¹ Article 3(3) of the Europol-US supplement agreement.

³⁹² See the operational agreements concluded between Europol and Albania, Bosnia and Herzegovina, Canada, Georgia Liechtenstein, Moldova, Montenegro, Republic of Serbia, and Ukraine.

³⁹³ Confront the operational agreements of Europol with Australia, Colombia, Iceland, Principality of Monaco, North Macedonia, Norway, and Switzerland.

to the respective mandate³⁹⁴. Europol and Interpol may exchange operational, strategic, and technical information and co-ordinate activities – such as the development of common standards, action plans, training and scientific research, and the secondment of liaison officers. The parties must consult each other on the implementation of the agreement and may exchange liaison officers according to the corresponding MoU. The information shall be processed for the sole purpose for which it was transmitted, according to their respective legal frameworks, and in no case can they process information obtained in violation of human rights. The information may be transmitted spontaneously or upon request. The exchange of information ‘revealing racial origin, political opinions or religious or other beliefs, or concerning health and sexual life’ must be limited to ‘absolutely necessary cases’ and only in addition to additional data, or by indicating the existence of additional data. The information may be subject to specifications and restrictions on its usage, access, restriction, and the condition of deletion or destruction of such information, before, at the moment of, or after the transmission. Onward transfers are permitted, subject to the prior consent of the other party, and under the legal framework of the transmitting party. If the information is available thanks to direct access to the database, the access shall be governed by specific rules and conditions applicable to the operation of the database in question. Indeed, as the EDPS noted, Article 2(m) of the Europol Regulation’s definition on personal data covers both push and pull systems³⁹⁵ and, with the former, Europol may be granted access to the databases or information systems of a national, Union, or international nature under the principle of reciprocity³⁹⁶. This is the case regarding Interpol’s global communication systems, SLTD and TDAWN, to which Europol has 24/7 access. The pull system raises special concerns regarding responsibility, as the controller owning the data remains responsible for the legality of the transfer and the accuracy of the data transmitted despite losing control over it. Thus, if Europol accesses data stored at national, Union, or international level, the respective national, Union, or international controller remains the only body accountable for the data processing activity according to the legislation regulating that access. In this case, Europol risks circumventing EU standards if the accessed database is subject to a level of protection that is not equivalent to that of the EU.

³⁹⁴ See Claudio Matera, “Police and judicial cooperation in criminal affairs” in Ramses A. Wessel and Jed Odermatt, *op cit.*, pp. 483-506.

³⁹⁵ Opinion of the EDPS on the *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA*, Brussels, 31.05.2013, p. 17: ‘[...] the communication of personal data, actively made available, between a limited number of identified parties, with the knowledge or intention of the sender to give the recipient access to the personal data’. With the latter pull system, Europol grants Eurojust, OLAF, and the Member States access to its data under a hit/no-hit mechanism.

³⁹⁶ Article 23(3) of the Europol Regulation.

It is crucial to highlight that Europol's mandate forbids it from receiving information from third parties in cases where the data was obtained 'in obvious violation of human rights'³⁹⁷ and this must also be applicable to the Europol-Interpol relationship. In this sense, the Europol-Interpol agreement requires transmitting data to the other party in compliance with an adequate level of protection of personal data. The receiving party, for its part, must decide whether to insert the information into its own files within a period of six months. Final dispositions concern the assessment of the reliability of sources of information, the ability to correct and delete information transmitted from one party to another, and the principle of confidentiality. The data subjects' rights are exercised before both parties that can consult each other before issuing a final decision. The settlement of disputes is the competence of an *ad hoc* Committee at the request of the Director of Europol or the Secretary General of Interpol, the Committee is made up of three members of the Management Board of Europol and three members of the Executive Committee of Interpol.

b) The transfer of personal data under the Europol Regulation

The European Commission has always looked at Europol's empowerment to conclude legal binding agreements with suspicion in light of the founding Treaty's provisions. Despite its "transformation" into an agency, Europol's rules regulating its external activity follows those of the Europol Convention, through which it could conclude treaties by virtue of its international nature. Notably, Europol's external activity was linked to the Council of the EU that: first, unanimously agreed upon the partners with which Europol could conclude an agreement following the agency's Management Board proposal and, second, approved their conclusion. In the *Europol* ruling³⁹⁸, the CJEU clarified that the Council's decision approving the list of third partners with which the Executive Director could have entered into negotiation³⁹⁹ stemmed from the executive powers of that institution rather than its legislative one⁴⁰⁰ by virtue of Article 26(2) of the Europol Decision. In the Court's words:

³⁹⁷ Article 23(9) of the Europol Regulation.

³⁹⁸ C-363/14, *European Parliament, represented by F. Drexler, A. Caiola and M. Pencheva, acting as Agents, with an address for service in Luxembourg, v Council of the European Union*, 10 September 2015, ECLI:EU:C:2015:579.

³⁹⁹ Article 23(2) of the Europol Decision and the following Council Decision 2009/935/JHA of 30 November 2009 determining the list of third States and organisations with which Europol shall conclude agreements, *OJ L* 325, 11.12.2009, pp. 12-13.

⁴⁰⁰ The former third pillar structure made it difficult to distinguish between legislative and executive powers since Article 39(1) of the 1997 TEU did not specify in which circumstances the Council was using one or the other one, except from the voting quorum that required the Council's unanimous or qualified majority vote.

‘[...] the inclusion of a third State on the list does not in itself allow any transmission of personal data to that State. [...] such transmission is possible only after the conclusion between Europol and the third State of an agreement specifically authorising the transmission of such data. It must be emphasised in this connection that [...] the negotiation and conclusion of such an agreement involves, after the inclusion of the third State on the list, successive decisions of the Europol Management Board and the Council, the former remaining free not to authorise the Director of Europol to enter into negotiations with the third State concerned, to direct those negotiations towards the conclusion of an agreement not permitting the exchange of personal data or finally not to approve the draft agreement negotiated by the director, and the latter remaining free not to approve the draft transmitted by Europol’⁴⁰¹.

Following the CJEU judgment, the Council started labelling its decisions with the adjective “implementing” but, arguably⁴⁰², it was not obliged to consult the European Parliament before adopting them. From this judgment Prof. Coman Kund maintains that Europol cooperation agreements should be classified as ‘international technical–administrative agreements’ following the Council’s executive powers, a distinction which does not necessarily encroach upon Article 218 TFEU⁴⁰³. The author elucidates that although the Lisbon Treaty changed the existing institutional *equilibrium* – first, because of the communitarisation of the third pillar policies and, second, because of the participation of the European Commission and the European Parliament in Article 218 TFEU –, the administrative-technical nature of Europol’s agreements means that they do not fall foul of Article 218 TFEU. In his words:

‘Europol’s cooperation agreements are in line overall with *Meroni* and do not seem to disturb the institutional balance in EU external relations. Being concluded by an EU body acting on the global level, Europol’s agreements are considered as being carried out ultimately on behalf of the European Union, which is in contrast with the Common Approach on EU agencies, stipulating that EU agencies cannot commit the Union to international obligations’⁴⁰⁴.

Indeed, the Europol Decision followed the Convention’s legislative procedure, which accepted Europol’s agreements as a treaty rather than an administrative agreement. Even accepting their executive character – the author takes for granted that Europol’s operational agreements are executive agreements⁴⁰⁵ concluded by the agency on behalf of the EU under

⁴⁰¹ C-363/14, *European Parliament, represented by F. Drexler, A. Caiola and M. Pencheva, acting as Agents, with an address for service in Luxembourg, applicant, v Council of the European Union*, para. 55.

⁴⁰² In C-540/13, *European Parliament v Council of the European Union*, 16 April 2015, EU:C:2015:224, the CJEU came to the conclusion that Article 18(2) of the Council Decision 2008/633 conferring to the Council the power to adopt a Council Decision with which the decision would have entered into force should have been interpreted in the light of Article 39(1) of the 1997 TEU that ensured the European Parliament to be consulted. See also the Council of the EU, *Information Note from the Council Legal Service, Judgments of the Court of Justice of 16 April 2015 in Cases C-317/13, C-540/13 and C-679/13 - Annulment of Council Decisions 2013/129/EU and 2013/496/EU (psychoactive substances) and Decision 2013/392/EU (date of effect of the VIS)*, 8541/15, Brussels, 4 May 2015.

⁴⁰³ Florin Coman-Kund, 2018, *op. cit.*, p. 31.

⁴⁰⁴ *Ibid.*, p. 32.

⁴⁰⁵ Fred L Morrison, *loc. cit.*

public international law, though this has been questioned in other works⁴⁰⁶ –, it is still unclear on which legal bases, both substantial and procedural, the Council could have delegated their conclusion to a Union agency. Could the Europol Decision legitimise the conclusion of an EU executive agreement that was undertaken on behalf of the Council by the agency? According to the analysis made in Chapter IV, we believe that the answer is “no”. Firstly, the principle of conferral requires a clear substantive legal basis to be found in the founding Treaties: We warned that Article 216 TFEU is misleading when it affirms that: ‘The Union may conclude an agreement with one or more third countries or international organisations where [...] is provided for in a legally binding Union act’ since this norm seems to enable the conferral of treaty-making powers to the EU through an act of secondary law, but the majoritarian doctrine discards this position⁴⁰⁷. Second, although the CJEU has not clarified if the delegation of executive treaty-making power is possible within the EU legal order, we also noted that the founding Treaties do not foresee any “simplified” procedure allowing for the conclusion of executive agreements as it does, for example, with the Member States. Prof. Coman-Kund notes that because of the control exercised by the Council, Europol’s agreements have bound the EU and not its institution(s), but the author does not put into evidence that the European Parliament’s lack of involvement must be considered as breaching Article 218 TFEU. The author takes for granted that the ‘informal and formal interactions between the agency and the Council, the Commission as well as the Member States’⁴⁰⁸, i.e. the simplified procedure through which Europol’s agreements were concluded, satisfies the principle of institutional balance before and after the entry into force of the Lisbon Treaty. However, Prof. Coman-Kund seems to shape his position together with Ott and Vos, who affirm:

‘Article 218 TFEU does not foresee that executive agreements exist without the consent by the European Parliament [...] The only exception to the participatory rights of the European Parliament will only be informed in case the legal basis does not refer to the ordinary or special legislative procedure or the agreement relates to the CFSP. Hence the current practice of Europol’s international cooperation breaches Article 218 TFEU by disregarding the European Parliament’s powers’⁴⁰⁹.

The picture is easier to resolve if we consider, as Prof. Coman-Kund does, that the (political) agreement between the European Commission, the European Parliament and the Council of the EU banned Union agencies from any ability to represent the EU on the external stage, and the

⁴⁰⁶ Andrea Ott, Ellen Vos, and Florin Coman-Kund, 2013, *op. cit.*, p. 29, puts it under discussion while affirming that: ‘[...] in the case of Europol it is doubtful whether these agreements are just technical agreements with reference to their content and aims, while it is moreover highly disputable whether such a practice of executive agreements is recognized in EU law’.

⁴⁰⁷ See Chapter II.

⁴⁰⁸ Florin Coman-Kund, 2018, *loc. cit.*

⁴⁰⁹ Andrea Ott, Ellen Vos, and Florin Coman-Kund, 2013, *loc. cit.*

conclusion of international agreements by Europol on the EU's behalf is inconsistent with this approach. A last “disturbing factor” we wish to highlight is that with operational agreements the adequacy assessment on the data protection system of the third party⁴¹⁰ was made by Europol itself, after consulting the Joint Supervisory Body and under the authorisation of the Management Board. This provision turns out to be incompatible with the current empowerment of the European Commission to adopt decisions on adequacy and, consequently, breaches the principle of institutional balance.

The new Europol Regulation does not contemplate the possibility to conclude either operational or strategic agreements to overcome speculations, which makes Europol's external action framework consistent with the Lisbon Treaty⁴¹¹ and the 2012 Joint Statement on decentralised agencies⁴¹². The Europol Regulation pays greater attention to data leakages from the EU – in this case from Europol – to third countries and international organisations, and as a result, the regime on the transfer of personal data is made of three distinct tools:

- an adequacy decision adopted by the European Commission by virtue of Article 36 LED;
- an international agreement concluded between the EU and a third country or international organisation pursuant to Article 218 TFEU offering adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals, or
- a cooperation agreement allowing for the exchange of personal data⁴¹³ that was concluded before 1 May 2017 in accordance with Article 23 of the Europol Decision⁴¹⁴.

Although the Europol Regulation makes safe cooperation agreements concluded before 1 May 2017, the European Commission is called on to assess ‘the provisions contained in the

⁴¹⁰ See Article 5(4) of the Council Decision 2009/934/JHA.

⁴¹¹ It might be noted that the Greek template structure existing before the Lisbon Treaty entered into force prevented the adoption of both a LED adequacy decision – implementing powers were indeed custodied by the Council – and a PJCCM international agreement – Member States retained the conclusion of PJCCM Conventions under the intergovernmental roof.

⁴¹² See *supra*.

⁴¹³ E.g., the Agreement between the US and the European Police Office of 6 December 2001, and Supplemental agreement between Europol and the US on exchange of personal data and related information, published on the website of Europol.

⁴¹⁴ See Article 25(4) of the Europol Regulation:

‘By 14 June 2021, the Commission shall assess the provisions contained in the cooperation agreements referred to in point (c) of paragraph 1, in particular those concerning data protection. The Commission shall inform the European Parliament and the Council about the outcome of that assessment, and may, if appropriate, submit to the Council a recommendation for a decision authorising the opening of negotiations for the conclusion of international agreements referred to in point (b) of paragraph (1)’.

cooperation agreements [...], in particular those concerning data protection' by 14 June 2021 in order to propose the conclusion of an international agreement if necessary. According to the European Commission, '[t]he Commission shall inform the European Parliament and the Council about the outcome of that assessment, and may, if appropriate, submit to the Council a recommendation for a decision authorizing the opening of negotiations for the conclusion of international agreements referred to in point (b) of paragraph (1)'⁴¹⁵. Following this regime, the European Parliament opposed the conclusion of some last-minute cooperation agreements with Brazil, Georgia, Mexico, and the United Arab Emirates by highlighting the inadequate level of protection of personal data in place in these countries⁴¹⁶.

In 2017, the European Commission asked the Council to undertake negotiations with Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia, and Turkey to conclude (binding) international agreements for the exchange of information in order to fight serious crimes and terrorism⁴¹⁷. Recital (35) of the Europol Regulation foresees that:

‘where appropriate and in accordance with Regulation (EC) No 45/2001¹⁴ the Commission should be able to consult the EDPS before and during the negotiation of an

⁴¹⁵ Article 25(4) of the Europol Regulation.

⁴¹⁶ Council of the UE, *Note from the Presidency, List of third States and organizations with which Europol shall conclude agreements*, 6473/14, Brussels, 17 February 2014.

⁴¹⁷ Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the Hashemite Kingdom of Jordan on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Jordanian competent authorities for fighting serious crime and terrorism, COM(2017) 798 final, Brussels, 20.12.2017; Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the Republic of Turkey on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Turkish competent authorities for fighting serious crime and terrorism, COM(2017) 799 final, Brussels, 30.10.2019; Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the Lebanese Republic on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Lebanese competent authorities for fighting serious crime and terrorism, COM(2017) 805 final, Brussels, 20.12.2017; Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the State of Israel on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Israeli competent authorities for fighting serious crime and terrorism, COM(2017) 806 final, Brussels, 19.12.2018; Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and Tunisia on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Tunisian competent authorities for fighting serious crime and terrorism, COM(2017) 807 final, Brussels, 21.12.2017; Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the Kingdom of Morocco on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Moroccan competent authorities for fighting serious crime and terrorism, COM(2017) 808 final, Brussels, 20.12.2017; Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the Arab Republic of Egypt on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Egyptian competent authorities for fighting serious crime and terrorism, COM(2017) 809 final, Brussels, 20.12.2017; Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the People's Democratic Republic of Algeria on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Algerian competent authorities for fighting serious crime and terrorism, COM(2017) 811 final, Brussels, 21.12.2017.

international agreement' between the EU and a third country to allow the exchange of data between Europol and the authorities of this third country'.

The EDPS complained of not having been consulted prior to the adoption of the European Commission's Recommendations. In Opinion No. 2/2018⁴¹⁸, the EDPS recalled that these agreements must comply with Article 52(1) of the CFREU so as to 'strike a fair balance between the need to fight serious crimes and terrorism and the sound protection of personal data and other fundamental rights' by conducting a country-by-country evaluation⁴¹⁹. Furthermore, in the absence of an adequacy decision, the EDPS recalled that the agreements should have not undermined the EU's constitutional principles for which third countries must comply with basic human rights and, at least, Articles 7 and 8 of the CFREU that safeguard the principles of: purpose limitation; the right to access and rectify personal data, and the provision of control exercised by an independent authority.

Despite the existence of specific provisions set forth in the Europol Regulation, the EDPS recalled that this regime must be interpreted in the light of the LED, Convention 108, and the Council of Europe's Recommendation No. R (87) 15. As a result, the EDPS recommended assessing the adequacy of the protection ensured by the third countries in question according to the criteria set forth in recital (71) of the LED and noted that, while some of the third countries had abolished the death penalty, others – namely, Morocco, Algeria, and Tunisia – had only adopted a moratorium, which raised concerns on their commitment in human rights matters. In addition, the EDPS warned that Europol and the information providers – e.g., the Member States – may share responsibilities in data processing activities which should have been reflected in the agreement⁴²⁰. It pointed out, for example, that the purposes for which data could be transferred should have been narrowly specified by listing the offences for which data could be shared, clarifying with which third countries Europol's Operational Analysis Projects could cooperate, and on what grounds the necessity and proportionality of the processing would have been based⁴²¹. On 30 October 2019, the European Commission issued a second

⁴¹⁸ Opinion of the EDPS No. 2/2018 on *eight negotiating mandates to conclude international agreements allowing the exchange of data between Europol and third countries*, Brussels, 14.03.2018.

⁴¹⁹ *Ibid.*, p. 7.

⁴²⁰ Article 18 Europol Regulation.

⁴²¹ Opinion of the EDPS No. 2/2018 on *eight negotiating mandates to conclude international agreements allowing the exchange of data between Europol and third countries*, Brussels, 14.03.2018, p. 11. Other suggestion concerned: the list of authorities in charge of receiving data; the prohibition of onward transfers; the specification of the existence of restrictions on the processing of personal data transferred; the establishment of an independent supervisory authority in foreign countries; the existence of enforceable subjective rights among which the right to access and rectify personal data as well as the right to information; the subjection of the transfer of sensitive data to the principles of strict necessity and proportionality and to 'solid justifications, based on grounds other than the protection of public security against terrorism and serious transnational crime' in the terms used by CJEU in *Opinion 1/15*, para. 165; the timeless communication by Europol to third countries of the erasure of personal data

Recommendation for a Council Decision authorising the negotiations of an agreement with the New Zealand, one of the states of the FVEY⁴²², on the exchange of personal data between Europol and the New Zealand authorities competent for fighting serious crime and terrorism⁴²³. In general terms, the EDPS welcomed the envisaged agreement as many of the suggestions previously made with regard to Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia, and Turkey had been incorporated⁴²⁴. Yet, a new recommendation was made to support this agreement, that is, the insertion of Article 16(2) TFEU as an additional substantive legal basis. Also, the EDPS invited the European Commission to list the criminal offences for which data could be shared on a case-by-case basis, to periodically review the respect of time-limit periods for storage, and to inform the data subject that their data was processed in order that they might exercise the right to rectification and erasure of personal data in New Zealand.

With the new Regulation, Europol's powers were been reduced to the adoption of working and administrative arrangements⁴²⁵, which seems to re-propose the old dichotomy of operational/strategic agreements since, at first sight, working arrangements cannot regulate the exchange of personal data while administrative arrangements can, notwithstanding whether this is supported by an adequacy decision, an international agreement, or an old cooperation agreement. Therefore, working arrangements are expected to cover cooperative relations, and administrative arrangements to implement Article 218 TFEU or an adequacy decision from the European Commission. Nevertheless, the nature of the working and the administrative arrangements is not so clear: regarding the former the Europol Regulation specifies that they must not bind the EU or the Member States⁴²⁶, but nothing is specified as far as administrative arrangements are concerned⁴²⁷. As the EDPS recalled, only 'legally binding instruments' ensured Europol's accountability *vis-à-vis* third parties and the EDPS urged to use these

in its system, and the accomplishment by the latter to the agreed data retention period; the provision of suspension or termination of the agreement in case of data breaches similarly to the regime set forth for adequacy decisions, and the insurance that data already shared will be continued to be processed in accordance with the agreement suspended or terminated.

⁴²² See Chapter I.

⁴²³ Europol and New Zealand had concluded working arrangement in April 2019 but this was not considered a valid legal basis for exchanging information.

⁴²⁴ Opinion of the EDPS No. 1/2020 on *the negotiating mandate to conclude an international agreement on the exchange of personal data between Europol and New Zealand law enforcement authorities*, Brussels, 31.01.2020.

⁴²⁵ Articles 25(1) and 32(4) of the Europol Regulation.

⁴²⁶ Article 23(4) of the Europol Regulation. With regard to the recent working arrangements concluded with Israel, Japan, and New Zealand, Florin Coman-Kund, 2018, *op. cit.*, p. 200, maintains that their content suggests having binding force contrary to what it may be thought at first. Also, these arrangements allow for the transfer of personal data based on the derogations foreseen in the Europol Regulation or allowed under the national legislation of the third country.

⁴²⁷ Their conclusion corresponds to the Management Board but is negotiated by the Executive Director – see Articles 11(1)(r) and 23(3) of the Europol Regulation.

instruments to conduct massive, structural, and repetitive transfer operations. In no case can the exchange of personal data⁴²⁸ be channelled through the so-called working arrangements due of their non-binding nature regarding Union bodies, the authorities of third countries and international organisations implementing international agreements and adequacy decisions⁴²⁹, or private parties⁴³⁰. However, according to the Europol Regulation, the agency can conclude administrative arrangements on mutual collaboration and the exchange of classified information, e.g. the ones signed with the General Secretariat of the Council⁴³¹ and with Interpol⁴³². As Prof. Coman-Kund recalls:

‘While on the face of it, the provisions of the new Regulation suggest that [administrative arrangements] would likely qualify as soft law measures [...], determining their legal nature requires a case-by-case analysis of each particular instrument in light of international law criteria’⁴³³.

For this reason, the author would have opted for further scrutiny on behalf of the institutions as well as the EDPS over the agency’s arrangements and he criticises the Europol Regulation through two observations. On the one hand, he observes that the agency’s operational priorities might be set aside, and, at the same time, he remarks that the negotiations will take even longer than the ones necessary to conclude a cooperation agreement, but that they come with an important advantage: the European Parliament must be asked to give its consent⁴³⁴. On the other hand, the author argues that it is not clear what kind of agreements the EU will conclude: they might be ‘special agreements’ on Europol’s cooperation with a third country or an international organisation, in particular with regard to exchanges of personal data, much like the current Europol’s cooperation agreements, or they might be broader framework agreements between the EU and the respective international partner covering various aspects of cooperation, including Europol’s goals. According to Coman-Kund: ‘Under the latter scenario, the

⁴²⁸ Article 23 of the Europol Regulation.

⁴²⁹ Article 25(1) last sentence of the Europol Regulation.

⁴³⁰ Article 34(4) of the Europol Regulation. Among the working arrangements concluded by Europol we shall mention the ones with: Chile; Israel; Japan; Kosovo; Mexico; New Zealand; OLAF; European Monitoring Centre for Drugs and Drug Addiction; EU military operation in the Southern Central Mediterranean; the EPPO; the Kosovo Specialist Chambers and Specialist Prosecutor’s Office, and Interpol with which Europol signed a MoU in 2003 on illegal immigration in the Mediterranean area and the terrorism domains.

⁴³¹ ‘The Secretary-General of the Council may use assessments submitted by Europol for all purposes in assisting the Council in determining the Union’s policy in the fight against terrorism’, in the Council of the EU Secretariat’s Note, *Framework for mutual collaboration and exchanging classified information between Europol and the General Secretariat of the Council*, 14050/05, Brussels, 7 November 2005.

⁴³² According to the Europol-Interpol operational agreement of 5 November 2001.

⁴³³ Florin Coman-Kund, 2018, *loc. cit.*

⁴³⁴ Article 11(2) of the Europol Regulation.

negotiation process might meet with specific difficulties depending on the breadth and complexity of the issues covered by such an agreement⁴³⁵.

As far as “soft” working arrangements are concerned, at the time of writing – March 2022 – Europol has concluded thirteen of them⁴³⁶, among which nine with third countries – the United Kingdom⁴³⁷, the Republic of San Marino⁴³⁸, New Zealand⁴³⁹, Mexico⁴⁴⁰, Kosovo⁴⁴¹, Japan⁴⁴², Israel⁴⁴³, Chile⁴⁴⁴, Andorra⁴⁴⁵ and Korea⁴⁴⁶ – and three with Union agencies, bodies, and offices – the European Union Naval Force Mediterranean (Operation Sophia)⁴⁴⁷, the European Monitoring Centre for Drugs and Drug Addiction⁴⁴⁸, and OLAF⁴⁴⁹. On closer inspection, these working arrangements foresee the possibility to exchange not only information – including specialist knowledge, general situation reports, specific operational reports, results of strategic analysis, and information on crime prevention methods and the participation in training activities – but also personal data through the designated National Contact Points⁴⁵⁰. Interestingly, some working arrangements – like the one signed by Europol and New Zealand – put special emphasis on the transfer of personal data from the third party to Europol and not the other way around. In this case, it is the third country that is called to support Europol by tracking down the information⁴⁵¹, for which we claim the implementation of a monitoring mechanism to verify that the data received is ‘not obtained in obvious violation of human rights’. Working arrangements do not replace existing Mutual Legal Assistance agreements,

⁴³⁵ Florin Coman-Kund, 2018, *op. cit.*, p. 17.

⁴³⁶ Consult Europol’s official website www.europol.europa.eu.

⁴³⁷ Europol-United Kingdom working arrangement of 23 September 2021, based on Article 577 of the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, *OJ L* 149, 30.4.2021, pp. 10-2539.

⁴³⁸ Europol-San Marino working arrangement of 22 September 2021.

⁴³⁹ Europol-New Zealand working arrangement of 17 April 2019.

⁴⁴⁰ Europol-Mexico working arrangement of 30 June 2020.

⁴⁴¹ Europol-Kosovo working arrangement of 27 July 2020.

⁴⁴² Europol-Japan working arrangement of 3 December 2018.

⁴⁴³ Europol-Israel working arrangement of 17 July 2018.

⁴⁴⁴ Europol-Chile working arrangement of 30 April 2021.

⁴⁴⁵ Europol-Andorra working arrangement of 24 September 2021.

⁴⁴⁶ Europol-Korea working arrangement of 23 December 2021.

⁴⁴⁷ Europol- European Union Naval Force Mediterranean working arrangement of 21 December 2018, replacing the previous MoU of 22 December 2015.

⁴⁴⁸ Europol- European Monitoring Centre for Drugs and Drug Addiction working arrangement of 6 December 2018.

⁴⁴⁹ Europol-OLAF working arrangement of 8 October 2020.

⁴⁵⁰ To be noted that the Europol-European Monitoring Centre for Drugs and Drug Addiction working arrangement excludes the conclusion of personal data – see Article 1.

⁴⁵¹ Article 10(4) of the Europol-New Zealand working arrangement.

cooperation agreements or arrangements, and ‘working law enforcement relationships’ concluded between the Union or its Member States and the other party. Yet, they enable the agency to directly exchange information with law enforcement authorities via the National Contact Points. Working arrangements agree that the exchange of personal data is regulated by each party’s respective legal frameworks⁴⁵² and they usually include provisions on:

- the restriction on the use, deletion, or destruction of the data;
- the deletion of unnecessary data if it had already been transmitted;
- the time-limit for retaining data necessary for the achievement of the purposes for which it was supplied⁴⁵³, the communication of corrected or deleted personal data to the other party;
- a general – yet derogable – clause prohibiting the communication of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and
- the processing of genetic data or data concerning a person’s health or sex life.

Also, Europol’s working arrangements establish that the information transmitted must be used only for that specific purpose and, finally, that any ‘onward transmission’ including to Union bodies, third countries, and international organisations must be previously authorised by the other party⁴⁵⁴. Notably, the working arrangements pay great attention to the reliability of the source from which the information comes, which enhances the agency’s scrutiny over the quality of the data processed; they also include detailed rules on data security in light of the principles of integrity and confidentiality of the data, without prejudice to the conclusion of

⁴⁵² To be noted that the Europol-OLAF working arrangement refers to Articles 19(2), 21(6) and (7), and 23(6) of the Europol Regulation.

⁴⁵³ In the case of the Europol-OLAF working arrangement, Article 9(4) establishes that the data transmitted by Europol and inserted in OLAF CMS must be retained according to the Commission Decision (EU) 2018/1962 of 11 December 2018 laying down internal rules concerning the processing of personal data by OLAF in relation to the provision of information to data subjects and the restriction of certain of their rights in accordance with Article 25 of the EUDPR. Moreover, OLAF is granted access to Europol’s data on the basis of a hit/non-hit mechanism by virtue of Article 21(1) of the Europol Regulation.

⁴⁵⁴ Different is the formulation used in the Europol-United Kingdom working arrangement for which: ‘Onward transmission of information provided by Europol shall be restricted to the competent authorities as referred to in Article 6, and shall take place under the same conditions as those applying to the original one’ – see Article 8(1). Besides, Article 17 foresees that the information transmitted previous to the entry into force of the working arrangement will be continued to be processed according to the conditions originally applicable ‘at the last moment prior to the data from which the Agreement was provisionally applied’. Also, Article 13(1) of the Europol-New Zealand is ambiguous since it enables onward transfer of information to ‘law enforcement authorities in New Zealand’ while affirming that: ‘Onward transmission of the information will be restricted to law enforcement authorities in New Zealand and will take place, at the initiative of NZP or at request of Europol, under the same conditions as those applying to the original transmission’. Thus, it is not excluded that foreign law enforcements present in New Zealand’s territory may be forwarded the information under Europol’s request – compare it with the Europol-Japan working arrangement, for example, whose Article 11(1) refers to ‘the law enforcement authorities of Japan’.

another arrangement on the parties' security organisation, and additional rules on education and training, standards of security screening, table of equivalences, handling of classified information and values of information assurance.

Now, the picture on Europol's external relations is further complicated if we consider that the Europol-San Marino, Europol-New Zealand, Europol-Mexico, Europol-Kosovo, Europol-Japan, Europol-Israel, Europol-Chile, Europol-Andorra, and Europol-Korea working arrangements set forth that they do not constitute a valid legal basis to transfer personal data from Europol to foreign authorities. Conversely, any transfer goes back to Articles 25(5) and 25(6) of the Europol Regulation, which in a very contradictory and controversial way means that it must be executed on a case-by-case basis or, exceptionally, in a 'set of transfers'⁴⁵⁵. These clauses derogate the general rule that prohibits the transfer of personal data without an instrument on adequacy or an agreement, so that 'they shall not be applicable to systematic, massive or structural transfers'⁴⁵⁶. Specifically, Article 25(5) of the Europol Regulation establishes that the Executive Director may authorise the transfer of personal data to third countries or international organisations on a case-by-case basis⁴⁵⁷ when it is:

- necessary in order to protect the vital interests of the data subject or of another person;
- necessary to safeguard the legitimate interests of the data subject where the law of the Member State transferring the personal data so provides;
- essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country;
- necessary in individual cases for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal sanctions, or
- necessary in individual cases for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection, or prosecution of a specific criminal offence or the execution of a specific criminal sanction.

However, the wording used in Article 25(5), second paragraph, of the Europol Regulation suggests that transfer of personal data is the rule rather than the exception. Hence, only when the Executive Director determines that the fundamental rights of the data subject override the public interest for the prevention, investigation, detection, or prosecution of criminal offences

⁴⁵⁵ Articles 23(4) and 25(1), last paragraph, of the Europol Regulation.

⁴⁵⁶ Article 25(5), third paragraph, of the Europol Regulation.

⁴⁵⁷ Article 25(5) of the Europol Regulation.

or the execution of criminal sanctions, or the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection, or prosecution of a specific criminal offence or the execution of a specific criminal sanction, then, the personal data could not be transferred⁴⁵⁸. Article 25(6) of the Europol Regulation is even more worrisome provided that it ends up legitimising systematic, massive, or structural transfers under the Executive Director's authorisation. According to this norm, Europol may forward "set of transfers" for period not exceeding one year 'taking into account the existence of adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals'⁴⁵⁹. Both the EDPS and the LIBE Committee⁴⁶⁰ called for significant clarification on what 'categories of personal data would include' any set of transfer. Indeed, it in case "set of transfers" enable the systematic, massive, or structural communication of personal data, then, we could argue that they do not constitute exceptional activities, as the co-legislators make them appear⁴⁶¹.

2.2. Eurojust's external relations

Following the Tampere Programme⁴⁶², the Council started debating the establishment of a unit made of national prosecutors, magistrates, or police officers of equivalent competence, to fight organised cross-border crime whose range of competences should have been aligned with those of Europol⁴⁶³. At the time, it was proposed to assign three main functions to the unit

⁴⁵⁸ Article 25(5), second paragraph, of the Europol Regulation.

⁴⁵⁹ Article 25(6) of the Europol Regulation.

⁴⁶⁰ Niovi Vavoula and Valsamis Mitsilegas, *Strengthening Europol's mandate: A legal assessment of the Commission's proposal to amend the Europol Regulation*, European Parliament's Committee on Civil Liberties, Justice and Home Affairs, Brussels, May 2021, p. 74. It must be noted that the position of the Council of the EU vis-à-vis the latest Proposal – see "Les États membres de l'UE adoptent leur mandat sur les nouvelles compétences dévolues à Europol", *Bulletin Quotidien Europe*, No. 12752, Brussels, 1.07.2021 – confirms the possibility for Europol to transfer personal data to a third country or 'third parties' in case an adequacy decision or an 'agreement' is missing 'but under very strict conditions and on the basis of a legal instrument guaranteeing the protection of these data' (our own translation). However, it is not clear which other 'legal instrument' can guarantee the protection of personal data under those conditions. According to the mandate agreed (our own translation):

'In order to ensure that Member States can effectively prevent the dissemination of terrorist content online, including in real time, Europol should be able to exchange personal data with private parties, including IP addresses or URLs linked to such content, necessary to assist Member States in preventing the dissemination of such content, in particular where such content is aimed at or has the effect of seriously intimidating a population and where there is an anticipated potential for exponential multiplication and virality across multiple online service providers'.

⁴⁶¹ Also, Article 25(6) clearly establishes that a set of transfers can be allowed for a period not exceeding one year which requires the EDPS to follow-up Europol's working arrangements in order to terminate or, if possible, renovate its clearances.

⁴⁶² See the Presidency Conclusions of the European Council in Tampere on 15 and 16 October 1999, para. 46.

⁴⁶³ On the evolution of the criminal judicial cooperation in the EU and its institutionalisation see Maria Esther Jordana Santiago, *El proceso de institucionalización de Eurojust y su contribución al Desarrollo de un modelo de cooperación judicial penal de la Unión Europea*, Madrid, Marcial Pons, 2018.

‘facilitating the proper coordination of national prosecuting authorities and [...] supporting criminal investigations in organised crime cases, notably based on Europol's analysis, as well as of cooperating closely with the European Judicial Network, in particular in order to simplify the execution of rogatory letters’⁴⁶⁴.

For these purposes, Pro Eurojust was established as a prototype unit that was replaced by Eurojust as soon as a Council Decision was adopted⁴⁶⁵. Moving under an intergovernmental roof, the adoption of a Decision⁴⁶⁶ pursuant to Article 34(2)(c) of the 1997 TEU was found to be the quickest method of bringing this about⁴⁶⁷ thereby conferring on Eurojust a *sui generis* form of governance made of National Members and a ‘College’⁴⁶⁸. Unlike other EU agencies Eurojust was conferred a centralised-vertical structure⁴⁶⁹ to:

- stimulate and improve coordination between the competent authorities of the Member States, and of investigations and prosecutions in the Member States, taking into account any request emanating from a competent authority of a Member State and any information provided by any body made competent by virtue of provisions adopted within the framework of the Treaties;
- improve cooperation between the competent authorities of the Member States, in particular by facilitating the execution of international mutual legal assistance and the implementation of extradition requests, and
- otherwise support the competent authorities of the Member States in order to render their investigations and prosecutions more effective⁴⁷⁰.

⁴⁶⁴ See the Presidency’s Note in Council of the EU, *Exploratory thoughts concerning EUROJUST*, 5700/00, Brussels, 4 February 2000.

⁴⁶⁵ See the Note from the General Secretariat in Council of the EU, *2001 Pro Eurojust Report*, 15545/01, Brussels, 20 December 2001.

⁴⁶⁶ Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, *OJL* 63, 6.3.2002, pp. 1-13. The Eurojust Decision had been amended by Council Decision 2003/659/JHA of 18 June 2003 amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, *OJL* 245, 29.9.2003, pp. 44-45, to manage the agency’s budget.

⁴⁶⁷ See the Note of the Portuguese, French, Swedish and Belgian delegations in Council of the EU, *Guidelines on Eurojust*, 7384/00, Brussels, 28 March 2000, p. 14. Nevertheless, the adaptation of Member States’ national laws was finally long and lead to fragmented domestic regimes – see the Council of the EU, *EUROJUST Annual Report 2006*, 7550/07, Brussels, 21 March 2007, p. 6, where it is maintained that Spain incorporated the Eurojust Decision in 2006 only while Greece had not done yet.

⁴⁶⁸ Articles 6 and 7 of the Eurojust Regulation. What Jordana Santiago, *op. cit.*, p. 129, defines as a ‘double hat’ nature because national authorities are also members of the Eurojust’s College.

⁴⁶⁹ Giovanni Barrocu, *La cooperazione investigativa in ambito europeo. Da Eurojust all’ordine di indagine*, Milano, CEDAM, 2017.

⁴⁷⁰ Article 3 of the Eurojust Decision.

Following the example of Europol, the Council proposed to insert references to Eurojust in the founding Treaties while devising the project on a Constitution for the EU⁴⁷¹ which was reflected in the Nice Treaty⁴⁷². The latter established Eurojust's empowerment in supporting criminal investigations against serious cross-border crime – particularly organised crime – taking into account the analyses carried out by Europol. On these bases, the Eurojust Decision was amended⁴⁷³ and Eurojust's operational tasks enhanced: competent authorities were to transmit the information to Eurojust⁴⁷⁴, among others, for the creation of the EU Terrorism Situation & Trend Report⁴⁷⁵, and thanks to the provision of an emergency cell for coordination that was to be made available 24/7⁴⁷⁶. In addition, Eurojust was mandated to resolve conflicts of jurisdiction by virtue of the Framework Decision 2009/948/JHA of 30 November 2009⁴⁷⁷ in order to find the State better positioned to take over a specific case⁴⁷⁸. Moreover, the new legal framework allowed Eurojust to progressively collaborate in Europol's AWFs according to the Eurojust-Europol administrative agreement⁴⁷⁹.

With the Lisbon Treaty, Eurojust's mandate was updated by virtue of Article 85 TFEU⁴⁸⁰ which fuelled a new institutional debate on the possibility to enhance Eurojust's

⁴⁷¹ See the Cover Note in Council of the EU, *IGC 2000: Incorporation of a reference to Eurojust in the Treaty*, CONFER 4806/1/00 REV 1, Brussels, 19 November 2000.

⁴⁷² Articles 29 and 31 of the 2002 TEU.

⁴⁷³ Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, *OJ L* 138, 4.6.2009, pp. 14-3.

⁴⁷⁴ Article 13 of the Eurojust amended Decision. The transmission of information was made through a "smart" PDF form available via the National Desks in the EU official languages – see the Council of the EU, *EUROJUST Annual Report 2011*, 8853/12, Brussels, 19 April 2012, p. 55 – but the non or late implementation of the Eurojust amended Decision seriously undermined the provision of such an obligation and, consequently, Eurojust pro-active activity.

⁴⁷⁵ The Eurojust amended Decision established a Eurojust National Coordination System according to Council Decision 2005/671/JHA, and it was in charge of transmitting reliable information to be included in the Eurojust CMS for which purpose it was granted access to, and of stimulating the exchange of information between Member States and Eurojust according to the latter's mandate – see María Esther Jordana Santiago, *op. cit.*, p. 138. Other strategic reports mentioned by the author are: the EU Organised Crime Threat Assessment; the Russian Organised Crime Threat Assessment; and the Organised Crime Threat Assessment on West Africa.

⁴⁷⁶ See Article 5a of the Eurojust amended Decision.

⁴⁷⁷ Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings, *OJ L* 328, 15.12.2009, pp. 42-47.

⁴⁷⁸ See for example Eurojust's assistance in a case of women trafficking from the Czech Republic to the United Kingdom in Council of the EU, 8853/12, Brussels, 19 April 2012, pp. 18 and 19.

⁴⁷⁹ *Ibid.*, p. 49, affirming that Eurojust was granted access to seventeen AWFs but still Member States refrained from giving it access to the ones on Islamist terrorism and domestic extremism.

⁴⁸⁰ Which includes Eurojust among the list of "privileged" agencies with a mandate established in the founding Treaties:

'1. Eurojust's mission shall be to support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime affecting two or more Member States or requiring a prosecution on common bases, on the basis of operations conducted and information supplied by the Member States' authorities and by Europol. In this context, the European Parliament and the Council, by means of regulations adopted in accordance with the ordinary legislative procedure, shall determine Eurojust's

‘Europeisation’⁴⁸¹. According to Aled Williams, former President of Eurojust and National Member of the United Kingdom, two main priorities had to be regulated in the new Eurojust Regulation:

‘[...] information flow between Eurojust and competent national authorities, which is a pre-condition for the reinforcement of the tasks and powers of Eurojust under Article 85(1) TFEU, and operational relationships – notably with the European Judicial Network, Europol and OLAF – that should be fostered both within and outside the EU’⁴⁸².

Article 85 TFEU was presented as a chance ‘to transform Eurojust from a simple mediator and player at horizontal co-operation level to a player with binding operational powers at vertical integration level’ while the new mandate should have been aligned with the institution of the EPPO⁴⁸³ in the fight against crimes affecting the EU’s financial interests⁴⁸⁴. However, Member States⁴⁸⁵ impeded the transformation of Eurojust into a supranational body entitled to

structure, operation, field of action and tasks. These tasks may include: (a) the initiation of criminal investigations, as well as proposing the initiation of prosecutions conducted by competent national authorities, particularly those relating to offences against the financial interests of the Union; (b) the coordination of investigations and prosecutions referred to in point (a); (c) the strengthening of judicial cooperation, including by resolution of conflicts of jurisdiction and by close cooperation with the European Judicial Network. These regulations shall also determine arrangements for involving the European Parliament and national Parliaments in the evaluation of Eurojust's activities. 2. In the prosecutions referred to in paragraph 1, and without prejudice to Article 86, formal acts of judicial procedure shall be carried out by the competent national officials’.

⁴⁸¹ For the analysis of Article 85 TFEU see María Esther Jordana Santiago, *op. cit.*, p. 204 ff., noting that: first, Eurojust is in charge of enhancing the criminal judicial cooperation in case of crimes affecting two or more Member States, notwithstanding its transborder nature, according to ‘common criteria’ that are not well definable; second, the agency is mainly conferred passive power consisting in coordinating investigations and prosecutions initiated under its initiative, and in strengthening the judicial cooperation – including the conflicts of jurisdiction – together with the European Judicial Network, with the exception of the power of initiative – directly or through the national competent authorities – of criminal investigations; third, Member States maintain intact their executive power of prosecution according to the second paragraph of Article 85 TFEU.

⁴⁸² Council of the EU, *Eurojust and the Lisbon Treaty: Towards more effective action Conclusions of the strategic seminar organised by Eurojust and the Belgian Presidency (Bruges, 20-22 September) - Information by the Presidency*, 17625/10, Brussels, 8 December 2010, p. 5.

⁴⁸³ According to Article 86 TFEU:

‘In order to combat crimes affecting the financial interests of the Union, the Council, by means of regulations adopted in accordance with a special legislative procedure, may establish a European Public Prosecutor's Office from Eurojust. The Council shall act unanimously after obtaining the consent of the European Parliament [...] The European Public Prosecutor's Office shall be responsible for investigating, prosecuting and bringing to judgment, where appropriate in liaison with Europol, the perpetrators of, and accomplices in, offences against the Union's financial interests, as determined by the regulation provided for in paragraph 1. It shall exercise the functions of prosecutor in the competent courts of the Member States in relation to such offences’.

On the difficult negotiations of the EPPO Regulation, see Giovanni Barrocu, *op. cit.*, 2017, pp. 75-99.

⁴⁸⁴ See the Meeting of the Consultative Forum of Prosecutors General and Directors of Public Prosecutions of the Member States of the European Union Eurojust, The Hague, 14 December 2012, as well as a summary of the replies to a questionnaire regarding Union’s financial offences in the Council of the EU, *Conclusions*, 8151/13, Brussels, 5 April 2013, p. 7, standing out Eurojust’s potential contribution in the Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union’s financial interests by means of criminal law, *OJL* 198, 28.7.2017, pp. 29-41, through the use of Joint Investigation Teams or Liaisons Magistrates to seal freezing and confiscation cooperation beyond the EU’s borders.

⁴⁸⁵ Professor Weyembergh in Council of the EU, 17625/10, Brussels, 8 December 2010, p. 11.

(full) operational competences⁴⁸⁶. They observed that neither Article 85 TFEU states that Eurojust's petition to initiate an investigation must be approved by the Member States, nor should Eurojust have the last word when issuing its opinion on a conflict of jurisdiction⁴⁸⁷. Eurojust's mandate was finally reformed in 2018 with Regulation (EU) 2018/1727 (or simply the Eurojust Regulation) that was adopted according to the ordinary legislative procedure⁴⁸⁸. From a governance perspective, the Eurojust's *sui generis* structure made of National Members, the College, and the Administrative Director was preserved⁴⁸⁹. Nevertheless, the College was endorsed with both operational and management functions and the structure was enriched by an Executive Board⁴⁹⁰ in line with the Joint Statement on decentralised agencies of 19 July 2012. Moreover, the European Commission was to be represented in the College while acting both as a Management Board⁴⁹¹ – that is, as far as non-operational functions are concerned – and as the Executive Director⁴⁹², though its presence was not really welcomed by the agency and the Coordinating Committee in the area of PJCCM. The latter proposed to expand the Eurojust Presidency team so as to include a representative from the Commission plus two other National Members (on rotation) in the new Executive Board⁴⁹³. As for its competences,

⁴⁸⁶ Such a transformation would have required the provision of legal remedies and judicial control against Eurojust's binding decisions, for example, on initiating judicial investigations and in resolving jurisdictional issues. See the Note from Eurojust in Council of the EU, *Strategic Seminar Eurojust: New Perspectives in Judicial Cooperation Budapest, 15-17 May 2011 Report*, 14428/11, Brussels, 21 September 2011, p. 4.

⁴⁸⁷ Article 4(2)(a) and (b) of the Eurojust Regulation maintains that Eurojust may ask competent authorities to: undertake an investigation or prosecution of specific acts, and accept that one of them may be in a better position to undertake an investigation or to prosecute specific acts. Eurojust is empowered to issue a written non-binding opinion in case Member States cannot agree on who should undertake an investigation or prosecution, as well as in case of recurrent refusals or difficulties concerning the execution of requests for, and decisions on, judicial cooperation, including requests and decisions based on instruments giving effect to the principle of mutual recognition. Nevertheless, in its third paragraph it is clarified that: 'The competent authorities of the Member States may refuse to comply with such requests [...] if doing so would harm essential national security interests, would jeopardise the success of an ongoing investigation or would jeopardise the safety of an individual'.

⁴⁸⁸ Differently from Article 86 TFEU that requires unanimity in the Council, previous consent of the European Parliament.

⁴⁸⁹ Also, the provision of a President and two Vice-Presidents its maintained according to Article 11 of the Eurojust Regulation, and the one of an Administrative Director that is elected by the College from a list of candidates proposed by the Executive Board – and not proposed by the European Commission as initially proposed – by virtue of Article 17.

⁴⁹⁰ Article 16 of the Eurojust Regulation. The Executive Board takes its decisions by majority of its members, and it is composed of: the President and Vice-Presidents of Eurojust, one representative of the Commission and two other members of the College designated on a two-year rotation system in accordance with Eurojust's Rules of Procedure. This implies that the Member States maintained the control over the decision-making procedure through their National Members gathered in the College. The Administrative Director, instead, attends the meetings of the Executive Board without the right to vote.

⁴⁹¹ Article 10(1)(b) of the Eurojust Regulation.

⁴⁹² Recital (19) of the Eurojust Regulation.

⁴⁹³ In these terms, the Executive Board could have preserved its administrative functions while relegating to the Council of Eurojust the agency's operational policy. See the Council of the EU, *Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (EUROJUST) - Orientation debate*, 9486/14, Brussels, 19 May 2014.

Eurojust can deploy cooperative and coordinative tasks concerning the serious crimes listed in Annex I of the Eurojust Regulation⁴⁹⁴. Among these activities⁴⁹⁵ we should recall that Eurojust may:

- request the setting up of a joint investigation team⁴⁹⁶, with or without Europol⁴⁹⁷, or participate in joint investigation teams with its national members;
- assist in the implementation of the European Arrest Warrant⁴⁹⁸;
- facilitate Mutual Legal Assistance through liaison magistrates⁴⁹⁹;
- ask Member States to undertake investigations⁵⁰⁰, and
- coordinate meetings⁵⁰¹ and centres⁵⁰².

The Member States' reluctance to regularly share their information with the EU⁵⁰³ means that Eurojust still merely deploys a supportive function for the exchange of information among

⁴⁹⁴ Article 3(1) of the Eurojust Regulation specifying that Eurojust should not exercise its competence in those cases for which the EPPO exercises its own.

⁴⁹⁵ Article 4 of the Eurojust Regulation.

⁴⁹⁶ Article 6(a)(iv) and Article 7(a)(iv) of the Eurojust Decision. Joint investigation teams were incorporated in the EU through the Council Framework Decision of 13 June 2002 on joint investigation teams, *OJ L* 162, 20.6.2002, pp. 1-3, following the non-ratification of several Member States of the Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union - Council Declaration on Article 10(9) - Declaration by the United Kingdom on Article 20, *OJ C* 197, 12.7.2000, pp. 3-23 – confront Article 13.

⁴⁹⁷ See the Hungarian Delegation in Council of the EU, *Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (EUROJUST) and the Proposal for a Regulation on the European Agency for Law Enforcement Cooperation (EUROPOL)*, 11682/14, Brussels, 9 July 2014.

⁴⁹⁸ Both in case of late or erroneous submission of a European Arrest Warrant request for which purposes Eurojust may be called to process European Arrest Warrants' personal data – see the Note from the General Secretariat in Council of the EU, *Second Annual Report of Eurojust (Calendar Year 2003)*, 8284/1/04 REV 1, Brussels, 26 April 2004, p. 13, and the contribution of Eurojust in the European arrest warrant proceeding highlighted in the Cover Note in Council of the EU, *Notifications to Eurojust of breaches of time limits in the execution of European Arrest Warrants (Article 17(7) (first sentence) of FD on EAW)*, 10270/14, Brussels, 26 May 2014.

⁴⁹⁹ Following the adoption of the Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union - Council Declaration on Article 10(9) - Declaration by the United Kingdom on Article 20, *OJ C* 197, 12.7.2000, pp. 3-23, replacing the European Mutual Assistance Convention of 10 April 1959 and its relevant Protocols.

⁵⁰⁰ Articles 6 and 7 of the Eurojust Decision: Eurojust has no initiative power to investigate or realise criminal proceedings in the Member States territories, but it may ask further competent authorities to join a specific case.

⁵⁰¹ Confront the Eurojust Rules of Procedure of 20 December 2019 available at www.eurojust.europa.eu. According to Prof. Jordana Santiago, *op. cit.*, p. 156, Eurojust coordinated meetings is the major source to exchange information.

⁵⁰² See the Council of the EU, 8853/12, Brussels, 19 April 2012, pp. 12 and 13. Coordination meetings '[...] bring together both law enforcement and judicial authorities from Member States and third States, allowing for strategic, informed and targeted operations in cross-border crime cases and the resolution of legal and practical difficulties resulting from the differences in the existing legal systems in the European Union'. Coordination centres, instead, 'ensure real-time transmission of information and coordination of measures between national authorities during a common action day' – see the Council of the EU, *EUROJUST Annual Report 2013*, 8151/14, Brussels, 25 March 2014, p. 20 ff.

⁵⁰³ See "Le Parlement européen donne un avis positif sur quatre décisions du Conseil sur les échanges automatisés de données", *Bulletin Quotidien Europe*, No.12918, 25.3.2022, on the transfer of DNA and dactyloscopic data as well as vehicle registration data in Italy and in Greece, and the Council of the EU, *Comments on Articles 9-26 of*

Member States by allowing them to integrate its infrastructure which enables the flow of information subject to previous authorisations⁵⁰⁴. Despite this, the communitarisation of the PJCCM area enhanced the Eurojust's presence in new investigatory instruments including: the European Investigation Order, for which purpose competent authorities could have used the European Judicial Network, Eurojust, or other channels used by judicial or law enforcement authorities⁵⁰⁵; and Directive 2014/41/EU of the European Parliament and of the Council to combat terrorism, where Eurojust was called on to resolve issues surrounding conflicts of jurisdiction in cases where a competent authority could not reach a consensus on an effective solution⁵⁰⁶. In addition, Eurojust's mandate is expected to be strengthened so as to contribute – together with the International Criminal Court – to the repression of the Ukrainian war by collecting, preserving, and sharing evidence of war crimes⁵⁰⁷. Although Eurojust has been granted access to only two over six large-scale IT systems⁵⁰⁸, it is called on to play a crucial role in the ECRIS-TCN to which it has been granted direct access. Indeed, Eurojust is designated as the contact point for third countries and international organisations that ‘may, for the purposes of criminal proceedings, address requests for information on which Member States, if any, hold criminal records information on a third-country national [...]’⁵⁰⁹. If while searching in the ECRIS-TCN Eurojust finds that a Member State holds criminal records of the third-country national at issue, it must inform the third party on how to address that Member State if, and only if, the Member State gives its consent. If no data is found, or the Member

the Draft Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust), 18169/13, Brussels, 21 January 2014.

⁵⁰⁴ See Article 21(2) of Eurojust Regulation. Note that during the negotiations, some delegations like Czech Republic opposed to granting Eurojust initiative powers – see the Council of the EU, *Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust) - Written comments by Czech Republic on Articles 1 - 21 of the Draft Regulation*, 13631/14, Brussels, 29 September 2014, p. 2.

⁵⁰⁵ Recital (13) of Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *OJ L* 130, 1.5.2014, pp. 1-36, substituting inter alia the Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence, *OJ L* 196, 2.8.2003, pp. 45-55, and the Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters, *OJ L* 350, 30.12.2008, pp. 72-92.

⁵⁰⁶ Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, *OJ L* 88, 31.3.2017, pp. 6-21 – confront Article 12.

⁵⁰⁷ “La commission européenne propose de renforcer le mandat d'Eurojust dans le contexte de crimes de guerre suspectés en Ukraine”, *Bulletin Quotidien Europe*, No. 12938, 26.4.2022. The Proposal or a Regulation of the European Parliament and of the Council amending Regulation (EU) 2018/1727 of the European Parliament and the Council, as regards the collection, preservation and analysis of evidence relating to genocide, crimes against humanity and war crimes at Eurojust, COM(2022) 187 final, Brussels, 25.4.2022, foresees: the implementation of a new automated data management and storage system, and the processing and sharing of data such as videos, audio recordings or satellite images.

⁵⁰⁸ Article 14(1) of the ECRIS-TCN Regulation and Article 49 of the Regulation 2018/1862.

⁵⁰⁹ Article 17 of the Eurojust Regulation.

State concerned does not give its consent, then, Eurojust must inform the third country or international organisation that it has completed the procedure ‘without providing any indication of whether criminal records information on the person concerned is held by one of the Member States’⁵¹⁰. The fact that Eurojust can receive requests for judicial cooperation turns the agency into a catalyst as far as international criminal judicial cooperation is concerned.

2.2.1. The processing of personal data by Eurojust

Ever since the Eurojust Council Decision, the agency has been assigned a ‘documentary database’ to provide legal and practical information to the Member States – as was previously done by the European Judicial Network⁵¹¹. Both the Index and the Temporary Work Files (TWFs) are held in the Eurojust CMS⁵¹² that was implemented thanks to the European Pool Against Organised Crime I Project for the Italian Direzione Nazionale Antimafia – partially founded by the EU Grotius II criminal programme – in order to create links among the different cases stored therein and to facilitate coordination⁵¹³. The software resulting from the E-POC project gave birth to Eurojust’s communication infrastructure. Although the case filing system was initially paper based, it was converted into a permanent IT system in 2004⁵¹⁴ under the

⁵¹⁰ Article 17(4) of the Eurojust Regulation.

⁵¹¹ Although not programmed at an initial stage, Eurojust’s tasks had been progressively coordinated with the one of European Judicial Network and, among others, it was granted access to its centralised information and telecommunication networks – see Article 26(2)(b) of the Eurojust Decision and the Guidelines on their practical relations in Copy Letter of the Presidency of the European Judicial Network in in Council of the EU, *Eurojust-EJN relations*, 1502/02, Brussels, 16 December 2002.

⁵¹² See the Cover Note in Council of the EU, *Proposal to the Council regarding rules of procedure on the processing and protection of Personal data at Eurojust*, 14439/04, Brussels, 12 November 2004, p. 19. The CMS was revised three times: first to adapt it to the Eurojust’s Data Protection Rules; second to support the investigation of terrorism, drug trafficking and trafficking in human beings and, finally, to develop the E-POC software and to enable the exchange of information with the Member States – see the Note from the Joint Supervisory Body in Council of the EU, *Activity Report of the Joint Supervisory Body of Eurojust for the year 2005*, 11875/06, Brussels, 24 July 2006, p. 7, and the in Council of the EU, *E-POC III and secure communications projects at Eurojust*, 5160/08, Brussels, 15 January 2008. The ‘E-POC IV’ was presented after the amendment of the Eurojust Decision to introduce a standardized model to exchange data among the different CMSs the Member States had implemented in the judicial domain – see the Eurojust’s Cover Note in Council of the EU, *Possible cooperation between Eurojust and the Council Working Party on Legal Data Processing (e-Justice) regarding the development of common standards for the exchange of data in the judicial domain*, 8991/10, Brussels, 30 April 2010. Later on, the CMS was upgraded twice: first, to increase the data processing speed and, second, to set up an e-mail management system that enables user to import link or large quantities of e-mail from the shared CMS mailboxes of the National Desks to the CMS – see the in Council of the EU, *EUROJUST Annual Report 2016*, 7971/17, Brussels, 5 April 2017, p. 19.

⁵¹³ See the Note from the General Secretariat in Council of the EU, 8284/1/04 REV 1, Brussels, 26 April 2004, p. 17.

⁵¹⁴ *Ibid.*, p. 23.

aegis of the governments' needs for information in order to combat terrorism and organised crime⁵¹⁵. The Eurojust CMS should:

- support the management, coordination, and prosecutions for which Eurojust provided assistance, in particular by cross-referencing information;
- facilitate access to information for on-going investigations and prosecutions, and
- facilitate the monitoring of the lawfulness of Eurojust's processing of personal data and its compliance with the applicable data protection rules⁵¹⁶.

National authorities are granted direct access to Eurojust's CMS and, therefore, to the Index and the TWFs⁵¹⁷. From the Eurojust Regulation we appreciate that the former, the Index, contains references to Eurojust's TWFs; the latter, the TWFs, are created by a National Member responsible for the storing and processing of the data inserted for every case according to Eurojust Regulation, or other applicable legal instruments⁵¹⁸. Access to the Index and the TWFs can be limited by the National Member that has introduced the data to the other National Members. The Index and the TWFs store different types of personal data: the Index contains the data listed in points (1)(a) to (i), (k) and (m) and (2) of Annex II; the TWFs, instead, gather all the personal data listed in Annex II, as well as non-personal data. The CMS can be connected to the secure telecommunications system of the European Judicial Network and can be accessed by the EPPO, though the information entered by the latter cannot be accessed at the national level. Notably, the Eurojust President proposed to upgrade the CMS in order to turn it into a 'system for data processing' that would include 'the pure registration of cases, but that could also support basic analysis by finding links between cases and entities, and include an advanced search tool and an easy tool dedicated to statistics'⁵¹⁹; yet, these functionalities should be accompanied by the corresponding empowerment of the agency, which Member States have

⁵¹⁵ See the Eurojust Note in Council of the EU, *EUROJUST report to Council on the scope for further measures to improve its capacity to contribute to fight against Terrorism*, 10008/04, Brussels, 1 June 2004.

⁵¹⁶ Article 23(2) of the Eurojust Regulation and the Eurojust report in accordance with the Council of the EU, *Article 16b of the Eurojust Decision*, 12582/13, Brussels, 19 July 2013, p. 4.

⁵¹⁷ See Article 22 of the Eurojust Regulation. For the storage of personal data see Article 29 of the Eurojust Regulation.

⁵¹⁸ Article 24 of the Europol Regulation. Specifically, the National Member inserting a new TWF shall identify potential Member States affected by the case at issue – and within its organization, the relevant authorities responsible for it – which may be registered by the College in its ordinary meeting as explained by María Esther Jordana Santiago, *op. cit.*, p. 153.

⁵¹⁹ Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust) - Invitation to Eurojust to provide a written contribution to the Working Party on Cooperation in Criminal Matters COPEN (Eurojust Regulation)*, 8488/14, Brussels, 4 April 2014, p. 39.

regularly opposed⁵²⁰. On 1 December 2021, as a part of the project on the digitalisation of justice in the EU⁵²¹, the European Commission advanced a new Proposal amending Eurojust's mandate as well as Council Decision 2005/671/JHA to modernise the agency's CMS, secure its communication channels, and implement a data communication tool⁵²². In addition, the European Commission proposed to fully integrate the Counter-Terrorism Register into Eurojust's CMS including the accompanying biometric data – i.e, fingerprints and facial images –, which requires an amendment to its mandate. We believe that this reform represents a step along the road toward the enhanced integration of Member States' cooperation in criminal judicial matters as the new Eurojust CMS is expected to store increasing amounts and types of data, and to cross-check and establish cross-links on the information stored therein.

Data protection principles are embedded in the Eurojust's CMS and the corresponding provisions are now inserted in the Eurojust Regulation⁵²³ to protect individuals and to encourage the Member States to share personal data with the agency. The harmonisation of data protection rules was perceived as a crucial element in enhancing the gathering and exchange of information⁵²⁴ and, unlike during the negotiations around the Eurojust Council Decision⁵²⁵, data

⁵²⁰ “Eurojust demande plus de moyens pour renforcer ses effectifs”, *Bulletin Quotidien Europe*, No. 12881, 2.2.2022.

⁵²¹ Commission Communication on the Digitalisation of justice in the European Union - A toolbox of opportunities, COM(2020) 710 final, Brussels, 2.12.2020.

⁵²² Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2018/1727 of the European Parliament and the Council and Council Decision 2005/671/JHA, as regards the digital information exchange in terrorism cases, COM(2021) 757 final, Brussels, 1.12.2021, p. 8.

⁵²³ Article 26 ff. of the Eurojust Regulation.

⁵²⁴ Council of the EU, *EUROJUST / ERA CONFERENCE 10 years of Eurojust Operational Achievements and Future Challenges The Hague, 12-13 November 2012 Outcome Report*, 8862/13, Brussels, 26 April 2013, p. 7 ff., focusing on two main data protection aspects: first, the confidentiality principles and the exercise of data subjective rights in the field of public documents' access and, second, the protection of personal data in the exchange of information.

⁵²⁵ Even if no provision on personal data was contemplated in the earliest debates of the Eurojust Council Decision – see the Addendum Cover Note from the Permanent Representative of the Federal Republic of Germany in Council of the EU, *Mr Wilhelm Schönfelder 12 May 2000 Secretary-General of the Council of the European Union, Mr Javier Solana Communication from the Federal Republic of Germany – Initiative by the Federal Republic of Germany regarding a Decision on setting up a EUROJUST team*, 8777/00 ADD 1, Brussels, 22 June 2000, p. 5, and further discussions in in Council of the EU, *Draft Council Decision setting up Eurojust with a view to reinforcing the fight against serious organised crime*, 13627/00, Brussels, 24 November 2000, p. 2, and in Council of the EU, *Draft Council Decision setting up EUROJUST*, 7408/2/01 REV 2, Brussels, 11 June 2001, p. 2 – the implementation of the CMS spurred the insertion of provisions on data protection in the Eurojust Council Decision, *inter alia*, because it enabled the exchange of information with third partners. Convention 108 of the Council of Europe was taken as a point of reference together with its 2001 First Additional Protocol: confront Articles 14, 15, 19, 20, 21, 22, 24, and 25 of the Eurojust Decision; the Note from the General Secretariat of the Council of the EU, *Bringing Member States' national law into conformity with the Decision setting up Eurojust – Discussion paper*, 9404/02, Brussels, 14 June 2002; the Note from the Presidency in Council of the EU, *Draft Council Decision setting up Eurojust*, 14052/00, Brussels, 4 December 2000, and the Joint Supervisory Body in Council of the EU, *Activity Report of the Joint Supervisory Body of Eurojust for the year 2008*, 12214/09, Brussels, 22 July 2009, p. 10. Regrettably, the Eurojust amended Decision did not make any reference to the DPF, but the EDPS recalled that this should have been applicable to Eurojust's activities consisting in the exchange of information with Member States – see the Opinion of the EDPS on *the Initiative of the Kingdom of Belgium, the*

protection occupied a prominent role in the debates over the Eurojust Regulation. At that time, the negotiations regarding the EU data protection package, together with the EPPO coordination norms and the norms on confidentiality, were still ongoing⁵²⁶. The special configuration of Eurojust was created so as to preserve a ‘tailor-made’ regime that, although aligned with the Europol and EPPO Regulations, should have maintained some unique elements. Eurojust is provided with a Data Protection Officer⁵²⁷ while the monitoring function deployed by national judges and independent authorities integrating the Joint Supervisory Body⁵²⁸ has shifted into the hands of the EDPS⁵²⁹ together with the competent national data protection authority⁵³⁰. The EDPS clarified that its supervisory power over the agency includes ordering the rectification, blocking, erasure, or destruction of data that would be processed in breach of the legislation, warning or admonishing the controller-EU body, imposing a temporary or definitive ban on the processing and, referring matters to the CJEU⁵³¹. This structure allows data subjects to submit a complaint directly to the EDPS that can then contact national supervisory bodies or the competent judicial body of the Member State from which the data originated or that it directly concerns⁵³². For this reason, the EDPS emphasised the necessity of the ‘structural involvement’ of the national supervisory authorities in the decision-making process. The possibility to seal

Czech Republic, the Republic of Estonia, the Kingdom of Spain, the French Republic, the Italian Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Poland, the Portuguese Republic, the Republic of Slovenia, the Slovak Republic and the Kingdom of Sweden with a view to adopting a Council Decision concerning the strengthening of Eurojust and amending Decision 2002/187/JHA, (2008/C 310/01), Brussels, 5.12.2008, paras. 22 and 23.

⁵²⁶ Council of the EU, *Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (EUROJUST) - Provisions relating to the European Public Prosecutor's Office*, 5730/15, Brussels, 2 February 2015, and *Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust) - Confidentiality and Security Rules (Articles 59 and 62)*, 5916/15, Brussels, 10 February 2015.

⁵²⁷ Articles 36-38 of the Eurojust Regulation specifying that the Data Protection Officer is independent in the exercise of its functions, though structurally linked to the College.

⁵²⁸ Established by Article 23 of the Eurojust Decision. The Eurojust Joint Supervisory Body firmly opposed to shifting the supervision role in the EDPS' hands and spurred the institution of a hybrid cooperation between the latter and national expertise in the judicial cooperation field – see, for example, the Council of the EU, *Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust) - Third Opinion of the Joint Supervisory Body of Eurojust*, 8638/15, Brussels, 8 May 2015.

⁵²⁹ Article 40 of the Eurojust Regulation.

⁵³⁰ The cooperation between the EDPS and data protection authorities is crucial provided that the former has no enforce powers over actors playing at national level, yet the Eurojust Joint Supervisory Body opposed to such an organisation while sustaining the maintenance of its powers – see the in Council of the EU, *Opinion of the Joint Supervisory Body of Eurojust regarding data protection in the proposed new Eurojust legal framework*, 17419/13, Brussels, 6 December 2013, p. 23.

⁵³¹ Opinion of the EDPS on *the package of legislative measures reforming Eurojust and setting up the European Public Prosecutor's Office ('EPPO')*, Brussels, 5.03.2014, p. 9, and the EDPS, *Monitoring and Ensuring Compliance with Regulation (EC) 45/2001. Policy Paper*, Brussels, 13.12.2010.

⁵³² Article 49 Eurojust Regulation.

the EDPS and national supervisory authorities' cooperation was channelled through the EDPB⁵³³ that hosts regular meetings with these stakeholders⁵³⁴.

In the Opinion delivered on 5 March 2015, the EDPS recalled that although the organisation consisted of prosecutors, judges, or police officers, Eurojust did not deploy a judicial function and it could not benefit from an exceptional data protection regime as is applicable, for example, to the CJEU⁵³⁵. Hence, its "assistance", "cooperation", "support" or "coordination" activity that aims at fostering cross-border cooperation in criminal investigations and prosecutions should have been regulated by the EU data protection rules. In the EDPS's words:

‘Since the activities of Eurojust cannot be assimilated to judicial activities *stricto sensu*, the processing of personal data by Eurojust should be subject to supervision by an independent supervisory authority, such as the EDPS’⁵³⁶.

The European Commission's Proposal regarding the Eurojust Regulation foresaw that the ECDPR should have been applicable to all of Eurojust's processing activities, yet the Eurojust Joint Supervisory Body highlighted that former third pillar activities fell outside the ECDPR and, consequently, Eurojust could have not been regulated by it⁵³⁷. The Eurojust Regulation should have aligned them with the Europol Regulation that distinguishes between 'administrative' and 'operational' personal data so that only the former fell within the scope of the ECDPR⁵³⁸ by virtue of the principle *lex specialis derogat legi generali*. Therefore, the Eurojust Regulation has been finally aligned with the new data protection package provisions⁵³⁹: while the process of 'administrative personal data unrelated to criminal investigations' is regulated by the general provisions of the EUDPR⁵⁴⁰, Chapter IX of the

⁵³³ Council of the EU, *Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust) - discussion paper on the Data Protection Supervision Regime for Eurojust*, 11993/17, Brussels, 11 September 2017.

⁵³⁴ Recital (41) of the Eurojust Regulation.

⁵³⁵ Specific reference was made on the basis of Article 46(c) of Regulation (EC) 45/2001 that excluded the CJEU judicial activity – see the Opinion of the EDPS on *the package of legislative measures reforming Eurojust and setting up the European Public Prosecutor's Office ('EPPO')*, Brussels, 5.03.2014, p. 6.

⁵³⁶ *Ibidem*.

⁵³⁷ Council of the EU, 17419/13, Brussels, 6 December 2013, p. 5.

⁵³⁸ It is significant Prof. Flore's distinction between operational and management functions: 'on the one hand, the "core business" of Eurojust namely judicial support for operational matters and strategic work; on the other hand, the "management" of Eurojust, involving the provision of administrative, executive or strategic support to the organisation' – see the Council of the EU, *Report from the Eurojust Seminar on the new draft Regulation on Eurojust: "an improvement in the fight against cross-border crime?"*, The Hague, 14-15 October 2013, 17188/1/13 REV 1, Brussels, 4 December 2013, p. 12, and the French position suggesting the specification of 'administrative' and 'operational' personal data in the light of two different regimes in the Council of the EU, *Comments on Articles 27-37 of the Draft Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust)*, 6981/14, Brussels, 7 March 2014, p. 7 ff.

⁵³⁹ Council of the EU, *Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust) - provisions on data protection (Presidency proposal)*, 10633/17, Brussels, 23 June 2017.

⁵⁴⁰ Recital (35) of the Eurojust Regulation.

EUDPR states that: ‘All processing of personal data by Eurojust, within the framework of its competence, for the fulfilment of its tasks should be considered as processing of operational personal data’⁵⁴¹. From the procedural rules on the processing of personal data⁵⁴², it is understood that the processing of personal data is regulated by two different regimes: one applicable to case-related data, and another one to non-case-related data. Only the former – the case-related data regime – concerns the data processing activities executed as part of Eurojust’s operational tasks, while the non-case-related data regime is aimed at regulating Eurojust staff members and ‘purely administrative information’ held by Eurojust⁵⁴³. Besides, within Eurojust’s operational activities a different treatment is foreseen for, on the one hand, the criminal investigation or prosecution of individuals⁵⁴⁴ and, on the other hand, witnesses or victims in a criminal investigation or prosecution⁵⁴⁵. As a general rule, Eurojust is entitled to process special categories of personal data such as that ‘[...] revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life’ not in the Index, but in the CMS and the TWFs; if this data refers to witnesses or victims, the decision to process them shall be taken by the National Members involved⁵⁴⁶.

2.2.2. The Eurojust’s cooperation agreements

a) The transfer of personal data through the Eurojust’s cooperation agreements

The first stage of Eurojust’s diplomatic activity was characterised by an intimate relationship with the EU’s institutions, especially the Council, due of the Member States’ willingness to control the agency’s operational activity⁵⁴⁷ and, to a lesser degree, the European Commission⁵⁴⁸. Soon after its establishment, Eurojust sealed a ‘practical arrangement’⁵⁴⁹ and a

⁵⁴¹ According to recital (34) of the Eurojust Regulation.

⁵⁴² Article 26(1) of the Eurojust Regulation: ‘This Regulation and Article 3 and Chapter IX of Regulation (EU) 2018/1725 shall apply to the processing of operational personal data by Eurojust. Regulation (EU) 2018/1725 shall apply to the processing of administrative personal data by Eurojust, with the exception of Chapter IX of that Regulation’, and previously, the Cover Note in Council of the EU, 14439/04, Brussels, 12 November 2004.

⁵⁴³ See the Addendum Cover Note in Council of the EU, *Proposal to the Council regarding rules of procedure on the processing and protection of Personal data at Eurojust*, 14439/04 ADD 2, Brussels, 28 January 2005.

⁵⁴⁴ Article 27(1) of the Eurojust Regulation.

⁵⁴⁵ Article 27(3) of the Eurojust Regulation.

⁵⁴⁶ Article 27(4) of the Eurojust Decision.

⁵⁴⁷ María Esther Jordana Santiago, *op. cit.*, p. 105 ff.

⁵⁴⁸ Articles 4 and 11 of the Eurojust Decision.

⁵⁴⁹ See the Cover Note in Council of the EU, *Draft agreement between Eurojust and Europol*, 15829/03, Brussels, 9 December 2003, so that Eurojust could have asked Europol to open a new AWF. The Agreement was signed on

MoU regarding classified information with Europol and further soft arrangements were celebrated with the OLAF⁵⁵⁰, the CEPOL⁵⁵¹ and the European Judicial Training Network⁵⁵².

After the humanitarian crisis of 2015, Eurojust has been progressively involved in the fight against migrant smuggling in cooperation with the other operational freedom, security, and justice agencies⁵⁵³. For example, the Eurojust amended Decision inserted a new reference to the EBCG Agency⁵⁵⁴. Eurojust also entertained endogamic relations with other strategic partners, including: the European Judicial Network; the Joint Investigation Teams Network; the European Network of contact points in respect of persons responsible for genocide, crimes against humanity and war crimes⁵⁵⁵; the European Monitoring Centre for Drugs and Drug Addiction⁵⁵⁶; the EU military operation in the Southern Central Mediterranean, and the Eulex Mission in Kosovo. It also took part in the International Association of Prosecutors, and in April 2007 it signed a Letter of Understanding on co-operation with the Office of the Prosecutor of the International Criminal Court based on ‘non-operational experiences’⁵⁵⁷.

The ability for Eurojust to conclude agreements with third countries and international organisations⁵⁵⁸, especially for the dispatch of associated liaison officers, was envisaged from

9 June 2004 and it is available at www.eurocrim.org. Although not explicated, from the wording of the Agreement it is understandable that it allowed the exchange of personal data – see for example Article 8.

⁵⁵⁰ With OLAF, Eurojust signed a practical agreement on 24 September 2008, and a MoU on 14 April 2003. The practical agreement contemplates the exchange of personal data. The MoU is not published; it includes the exchange of information, though we don’t know whether it contains personal data too – see the European Commission, “Olaf and Eurojust sign memorandum of understanding”, *Press Release*, Brussels, 14 April 2003.

⁵⁵¹ Eurojust-CEPOL of October 2009. Yet, the MoU does not provide for the exchange of personal data.

⁵⁵² Council of the EU, *EUROJUST Annual Report 2009*, 8147/10, Brussels, 30 March 2010, pp. 38 and 39. Eurojust- European Judicial Training Network MoU of 7 February 2008.

⁵⁵³ ‘Eurojust worked closely with Europol, Frontex and EASO to gather information on smugglers’ *modi operandi*, to support national authorities in tracing money, and to assist in investigations’, in Council of the EU, *EUROJUST Annual Report 2015*, Brussels, 7492/16, 4 April 2016, p. 31.

⁵⁵⁴ Article 26(3) of the Eurojust amended Decision sets forth: ‘in accordance with its mandate and tasks under point (m) of Article 8(1) of the EBCG Agency 2016 Regulation while specifying that ‘[t]he European Border and Coast Guard Agency’s processing of any personal data in connection therewith shall be regulated by Regulation (EU) 2018/1725’. The Eurojust-EBCG Agency MoU of 18 December 2013, was substituted by the Eurojust-EBCG Agency MoU of 18 December 2018. None of these two MoUs provide for the exchange of operational personal data.

⁵⁵⁵ Council of the EU, 8853/12, Brussels, 19 April 2012, p. 46 ff. The European Network of contact points in respect of persons responsible for genocide, crimes against humanity and war crimes (Genocide Network) was set up by the Council Decision 2002/494/JHA and reaffirmed by the Council Decision 2003/335/JHA and it is hosted by the own Eurojust.

⁵⁵⁶ Council of the EU, *Approval by the Council of the EU of the draft Memorandum of Understanding on cooperation between Eurojust and the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)*, 7628/14, Brussels, 14 March 2014. The Eurojust- European Monitoring Centre for Drugs and Drug Addiction MoU of 14 July 2014, does not foresee the exchange of personal data.

⁵⁵⁷ Council of the EU, *EUROJUST Annual Report 2007*, 6866/08, Brussels, 29 February 2008, p. 10.

⁵⁵⁸ Despite the increasing trend in collaborating with private parties in the frame of the criminal judicial cooperation, Eurojust’s mandate had not been adapted so as to enable it to cooperate with private parties though we can assume that the agency benefits from their cooperation ‘indirectly’ thanks to the strict cooperation it has been tailoring with Europol with which it sealed a cooperation agreement on 1 January 2010. Eurojust supports

the very beginning of the negotiations of the Eurojust Council Decision⁵⁵⁹ that conferred on it a ‘legal personality’⁵⁶⁰ and the power to deal with third countries regarding the secondment of liaison officers or liaison magistrates to Eurojust – including the exchange of personal data⁵⁶¹ – for which purpose Eurojust should have given precedence to states candidate to accessing the EU as well as to those countries with which Europol had already concluded an agreement with⁵⁶². Notably, the Eurojust Council Decision set forth that the third country should have had adhered to Convention 108 of the Council of Europe, or that it must have ensured an adequate level of protection⁵⁶³, except from those cases in which Eurojust could have taken ‘urgent measures to counter imminent serious danger threatening a person or public security’ following the recipient’s commitment that the personal data would be processed only for the purposes it had been transferred for⁵⁶⁴. Therefore, the conclusion of an administrative agreement with third countries and international organisations was submitted to ‘fact-finding missions’ to assess the implementation of data protection legislation in foreign territories⁵⁶⁵. In case of a non-adherence to Convention 108, the decision concerning the transfer of personal data was taken by the National Member concerned after consulting the Eurojust Data Protection Officer and, depending on the difficulty of the assessment, its Joint Supervisory Body as well⁵⁶⁶. Eurojust’s partners might include:

Europol in stimulating the flow of information from national authorities to Europol, and to share general and strategic analysis findings with it. Although Europol is not allowed to directly match its information with the one stored by Eurojust, the latter is required to do it on its behalf and to forward to Europol not only the data matched but also the “linked data”. Besides, Eurojust has to provide Europol with information related to its AWFs, falling within its fields of competences, on a regular basis; it may request Europol to open a new AWF or to establish a target group, and it is informed of any new AFW opened by Europol on its own. In parallel, Europol may ask Eurojust to intervene in coordinating AWFs, supporting the execution of a European arrest warrant or other instruments based on MLA and mutual recognition, and to coordinate the simultaneous investigative and judicial activities

⁵⁵⁹ See the Council of the EU, *Council Decision on setting up a EUROJUST team*, 8938/00, Brussels, 19 June 2000, p. 5.

⁵⁶⁰ Although it does not confer to Eurojust the title of subject of international law, Eurojust benefits from a certain degree of international subjectivity according to Mirentxu Jordana Santiago, “La dimensión exterior de Eurojust: medios de actuación y mecanismos de control”, in Montserrat Pi Llorens and Esther Zapater Duque, *La dimensión exterior de las agencias del espacio de libertad, seguridad y justicia*, Madrid, Marcial Pons, 2014, pp. 69-88.

⁵⁶¹ Article 27(3) of the Eurojust Decision. In the absence of an agreement, instead, personal data could have not been forwarded to third parties.

⁵⁶² Recital (15) of the Eurojust Decision. Therefore, Eurojust’s priorities started focusing on East partners – like the Russian Federation and Ukraine – Albania, Bosnia and Herzegovina, Cape Verde, Israel, Montenegro, Serbia, Turkey, and Latin America countries – namely, Brazil, Colombia, and Mexico. Also, the agency held strategic seminars with Southern Neighbours– Algeria, Egypt, Israel, Jordan, Lebanon, Libya, Morocco, Palestinian Authority, and Tunisia – the USA and the Western Balkans States – see the Council of the EU, *EUROJUST Annual Report 2012*, 8179/13, Brussels, 8 April 2013, p. 72.

⁵⁶³ Article 27(4) of the Eurojust Decision.

⁵⁶⁴ Article 17(6) of the Eurojust Decision.

⁵⁶⁵ See the Council of the EU, 8853/12, Brussels, 19 April 2012, p. 54.

⁵⁶⁶ See the Council of the EU, 14439/04, Brussels, 12 November 2004, p. 3.

- bodies competent by virtue of provisions adopted within the framework of the Treaties;
- international organisations and bodies, and
- authorities of third states competent for investigations and prosecutions⁵⁶⁷.

The Eurojust amended Decision introduced new provisions on Eurojust's cooperation with EU- and non-EU-related bodies through: first, the deployment of liaison magistrates appointed by Eurojust in third countries and international organisations⁵⁶⁸; second, the execution of foreign judicial cooperation requests⁵⁶⁹. Alongside liaison magistrates deployed in third countries – that must be subjected to a working arrangement with the authority of that third country and under the EDPS' supervision⁵⁷⁰ – and liaison prosecutors seconded at Europol's headquarter, Eurojust's external relations are further enriched by: participating in joint investigation teams; receiving foreign requests of judicial cooperation (especially of Mutual Legal Assistance) if these require execution in at least two Member States⁵⁷¹, and establishing Contact Points for the Member States through Eurojust in third countries⁵⁷². As a result, the amended Decision clarified that Eurojust could enter into administrative negotiations with, on the one hand, third countries and international organisations – through the so-called cooperation

⁵⁶⁷ Article 27(1) of the Eurojust Decision.

⁵⁶⁸ Article 26a of the Eurojust amended Decision.

⁵⁶⁹ Article 27a of the Eurojust amended Decision. See the Council of the EU, *Note to Initiative, Slovenia, the French Republic, the Czech Republic, the Kingdom of Sweden, the Kingdom of Spain, the Kingdom of Belgium, the Republic of Poland, the Italian Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Slovak Republic, the Republic of Estonia, the Republic of Austria and the Portuguese Republic* 7 January 2007, 5038/08, Brussels, 30 January 2008, p. 26:

‘The most basic situation, as set out in paragraph 2, is that in which Eurojust receives requests from a third State directly. This is only possible if the relevant international rules provide for this possibility. Initially, this will rarely or never be the case. Existing bilateral judicial assistance agreements between the Member States and third countries doubtless contain no such rules at the moment, nor do judicial assistance agreements already signed between the European Union and third States (e.g. the United States, Iceland and Norway). But the rule could be inserted in future agreements’.

⁵⁷⁰ Article 53 of the Eurojust Regulation.

⁵⁷¹ Article 54 of the Eurojust Regulation.

⁵⁷² See the Council of the EU, *EUROJUST Issue in focus number 3 - Cooperation with third States*, 5993/15 ADD 3, Brussels, 19 February 2015, p. 6, indicating that these countries are invited to Eurojust's cooperation meetings.

agreements – and, on the other hand, EU institutions, bodies, and agencies⁵⁷³ – through the working arrangements⁵⁷⁴.

Among the former group, the amended Decision expressly provided that Eurojust could cooperate with third countries and three specific types of organisations, namely⁵⁷⁵:

- international organisations and their subordinate bodies governed by public law;
- other bodies governed by public law which is based on an agreement between two or more States, and
- Interpol⁵⁷⁶.

In sum, Eurojust has concluded twelve cooperation agreements with third countries⁵⁷⁷ – namely Albania⁵⁷⁸, Montenegro⁵⁷⁹, North Macedonia⁵⁸⁰, Serbia⁵⁸¹, Georgia⁵⁸², Iceland⁵⁸³, Liechtenstein⁵⁸⁴, Moldova⁵⁸⁵, Norway⁵⁸⁶, Switzerland⁵⁸⁷, Ukraine⁵⁸⁸, and the US⁵⁸⁹. It also

⁵⁷³ Article 26(1) of the Eurojust amended Decision. As far as other EU bodies and institutions are concerned, the Eurojust amended Decision maintained a provision on the exchange of information between Eurojust and Europol – see the Eurojust-Europol Agreement of 1 January 2010 which includes the exchange of operational personal data as it is understandable from Article 13 for example; OLAF – Eurojust-OLAF practical agreement of 24 September 2008, the agreement includes the exchange of operational personal data according to the Point 6, and the Joint Situation Centre. Article 26(3) of the Eurojust amended Decision made a new reference to the EBCG Agency for which: ‘in accordance with its mandate and tasks under point (m) of Article 8(1) of the EBCG Agency 2016 Regulation while specifying that ‘[t]he European Border and Coast Guard Agency’s processing of any personal data in connection therewith shall be regulated by Regulation (EU) 2018/1725’. The Eurojust-Frontex MoU of 18 December 2013 was substituted by the Eurojust-EBCG Agency MoU of 18 December 2018. None of these two MoUs provide for the exchange of operational personal data.

⁵⁷⁴ Article 26a(2) of the Eurojust amended Decision.

⁵⁷⁵ Article 26a(1) of the Eurojust amended Decision.

⁵⁷⁶ See the Council of the EU, *Approval by the Council of the EU of the draft Memorandum of Understanding between Eurojust and INTERPOL*, 11602/13, Brussels, 27 June 2013, concerning the exchange of strategic information but not operational data or personal data – see the MoU on cooperation between Eurojust-INTERPOL of 15 July 2013.

⁵⁷⁷ Nevertheless, Eurojust has far more numerous contact points deployed in third countries – the Council of the EU, 6866/08, Brussels, 29 February 2008, p. 61 –, recalls Albania, Argentina, Bosnia & Herzegovina, Canada, Croatia, Egypt, FYROM, Iceland, Israel, Japan, Liechtenstein, Moldova, Mongolia, Montenegro, Norway, Russian Federation, Serbia, Singapore, Switzerland, Thailand, Turkey, Ukraine and USA – and it hosts ‘study visits’ – e.g., with Japan and Korea, *ibidem*, p. 63.

⁵⁷⁸ Eurojust-Albania Agreement of 5 October 2018. All the agreements referred to hereinafter are available at the same webpage.

⁵⁷⁹ Eurojust-Montenegro Agreement of 5 March 2016.

⁵⁸⁰ Eurojust-Yugoslav Republic of Macedonia of 28 November 2008.

⁵⁸¹ Eurojust-Republic of Serbia of 12 November 2019.

⁵⁸² Eurojust-Georgia of 29 March 2019.

⁵⁸³ Eurojust-Republic of Iceland Agreement of 2 December 2005.

⁵⁸⁴ Eurojust-Lichtenstein Agreement of 7 June 2013.

⁵⁸⁵ Eurojust-Moldova Agreement of 10 July 2014.

⁵⁸⁶ Eurojust-Norway Agreement of 28 April 2005.

⁵⁸⁷ Eurojust-Switzerland Agreement of 27 June 2019.

⁵⁸⁸ Eurojust-Ukraine Agreement of 27 June 2016.

⁵⁸⁹ Eurojust-US Agreement, 6 November 2006. The Agreement was found to be ‘challenging and problematic, particularly in the area of data protection’, in the Council of the EU, 7550/07, Brussels, 21 March 2007, p.7.

enhanced its contact points with the Organisation of American States, the Council of Europe's Group of States against Corruption⁵⁹⁰, and it underpinned important cooperation activity with the IOM under the aegis of the regional project Strengthening the Fight against Trafficking in Persons and Migrant Smuggling in the Western Balkans. Indeed, although Eurojust is not present in hotspot areas, it 'has established dedicated judicial contact points in Greece and Italy to support the Hotspots and to channel relevant information and cases to Eurojust's National Desks for judicial follow-up and coordination at EU level'⁵⁹¹. Eurojust concluded a MoU with La Red Iberoamericana de Cooperación Judicial⁵⁹² and another one with the United Nations Office on Drugs and Crime⁵⁹³ for the exchange of non-operational information. A MoU with the Interpol⁵⁹⁴ is also in place, and although it could have made its external relations with other international organisations, such as the World Customs Organisation⁵⁹⁵, official, Eurojust has not done so for the moment.

All these agreements – except for the that with the US which refers to the 'respective laws concerning the processing of personal data exchanged pursuant to [the] Agreement'⁵⁹⁶ – regulate the exchange of information, including personal data, taking as references the Convention 108 of the Council of Europe, Eurojust Council Decision's dispositions, and Eurojust's Rules of Procedure. In this sense, personal data must be processed: fairly; in a way not excessive to attainment of a specific goal; with a period of storage as long as required to achieve the goal for which data was processed according to the agreement, while bringing to the attention of the receiving party the existence of inaccurate personal data. Among the different channels for the transmission of the information, cooperation agreements reference: the liaison prosecutors⁵⁹⁷; the Contact Points for Eurojust, and the National Member concerned

⁵⁹⁰ See Juan Antonio García Jabaloy, "La dimensión exterior de Eurojust: una visión desde la práctica", Montserrat Pi Llorens and Esther Zapater Duque, *op. cit.*, pp. 89-100, p. 94.

⁵⁹¹ Council of the EU, 7971/17, Brussels, 5 April 2017, p. 26.

⁵⁹² Which improved the execution of extradition requests between the Member States and Latin America, see the Council of the EU, 8853/12, Brussels, 19 April 2012, p. 54. Another crucial network to fight drug trafficking is the Meetings of Ministers of Justice or Other Ministers or Attorneys General of the Americas (REMJA) – see the Council of the EU, 5993/15 ADD 3, Brussels, 19 February 2015, p. 14.

⁵⁹³ Council of the EU, 8147/10, Brussels, 30 March 2010, pp. 8 and 9.

⁵⁹⁴ Eurojust-Interpol MoU of 15 July 2013.

⁵⁹⁵ Articles 26 and 26a of the Eurojust amended Decision.

⁵⁹⁶ Article 9 of the Eurojust-US Agreement of 6 November 2006.

⁵⁹⁷ Liaison prosecutors are third countries authorities seconded at Eurojust's headquarter according to an underlying cooperation agreement. At the time of writing, the following states have seconded Liaison prosecutors to Eurojust, namely Albania, Georgia, Montenegro, North Macedonia, Norway, Serbia, Switzerland, Ukraine, the United Kingdom and the United States of America. If the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2018/1727 of the European Parliament and the Council and Council Decision 2005/671/JHA, as regards the digital information exchange in terrorism cases, COM(2021) 757 final, Brussels, 1.12.2021, is adopted, liaison prosecutors will be granted access to the CMS.

or the College; the liaison magistrates – with the sole exception of the Eurojust-US agreement⁵⁹⁸ – and the possibility of direct contact between the judicial authorities in charge of investigating and/or persecuting and/or carrying out the criminal proceedings and the National Members concerned, or the College. Regarding the latter case, the liaison officer or the Eurojust liaison magistrate should have been informed about the information exchange. In any case, the transfer of data revealing ‘racial or ethnic origin, political opinions or religious beliefs, trade union membership or concerning health and sexual life’ might occur if it is strictly necessary in order to attain the purposes of the agreement – or if the transfer would be considered ‘particularly relevant’ in the case of the Eurojust-US agreement⁵⁹⁹ that also lays down a list of limitations to its usage to protect personal and other data⁶⁰⁰ – however, the parties must have taken appropriate safeguards, such as security measures, to address the ‘special sensitivity’ of this data.

Eurojust cooperation agreements regulate data subjects’ rights and guarantees: the right to information and access to personal data, as well as the right to the correction, blockage, and deletion of personal data. The right to access personal data is developed in further detail in the latest cooperation agreements that set forth that it has to be exercised according to the law of the party to whom the data is transmitted and may be restricted in case its use jeopardises:

- the purposes of the processing;
- investigations, prosecutions, and criminal proceedings conducted by the competent authorities of the third party or of the concerned Member State, or
- the rights and freedom of the third parties.

In any case, the party from which the information is requested and the receiving party must be given the possibility to express their opinion and, specifically, they may allege the existence of grounds for denying access. Notably, the Eurojust-US agreement inserts an *ad hoc* provision on transparency⁶⁰¹ that safeguards the parties’ obligations to provide the data subjects with information concerning the identity of the controller, the recipients or categories of recipients, the existence of the right to access, the right to the rectification of data and further information on: the legal basis of the processing activity; the time limits for storing the data, and the right to recourse. The communication of these types of information might be limited in a similar manner to the restrictions on the right to access personal data. In addition, the existence of ‘the right to release of information’ is made safe with regard to the transmitting party. Eurojust

⁵⁹⁸ Confront Article 8 of the Eurojust-US Agreement of 6 November 2006.

⁵⁹⁹ Article 11 of the Eurojust-US Agreement of 6 November 2006.

⁶⁰⁰ Article 10 of the Eurojust-US Agreement of 6 November 2006.

⁶⁰¹ Article 14 of the Eurojust-US Agreement of 6 November 2006.

agreements pay attention to the data security principle and impose on the parties the duty to ensure the existence of ‘technical and organizational measures [...] against accidental or unlawful destruction, accidental loss or unauthorised disclosure, alteration, access or any unauthorised form of processing’. Besides, onward transfers are allowed only with the consent of the other party, and with appropriate safeguards regarding the protection of personal data. In case of damages caused to an individual for legal or factual errors in the exchange of data with Eurojust, the liability would lie with the third country and it is barred from claiming that Eurojust is responsible for transmitting inaccurate data⁶⁰². Eurojust, for its part, is responsible for legal and factual errors as a result of data erroneously communicated by it or one of the Member States to the third country, and it shall reimburse, upon request, the amount of money paid by the third country as compensation. However, if the compensation is due to the third country’s failure to comply with its obligations, then, the latter shall repay Eurojust upon request. In general, Eurojust’s agreements provide for an arbitrary dispute settlement mechanism – except the agreement with the US – the decision of which shall be considered as final and binding. In case of dispute, they impose the obligation to compensate on the other contracting party – the Member States or the third country in question – for the injury caused. Other agreements, instead, establish that any dispute should only be resolved through consultations and negotiations. Agreements can be terminated if the contracting parties wish so, while their entry into force depends on a notification of the successful ratification of the agreement to the other party, though no publication in the *OJ* is needed. Moreover, the monitoring of the implementation of the data protection and data security norms are undertaken by the Eurojust Data Protection Officer, the third country Data Protection Officer, and the Eurojust Joint Supervisory Body, according to the majority of the agreements, with the sole exception of those with Switzerland and the US.

It must be noted that the manner in which Eurojust concluded its agreements did not follow Article 30 of the 1997 TEU which regulates the conclusion of international agreements in the former third pillar structure. The Eurojust amended Decision imposed on the agency the duty to send a notification to the Council to explain the reasons for concluding an agreement with one of the partners on the list of priority of countries and international organisations approved by the College. Within two months the Council must have green light to the negotiations, or not⁶⁰³. Eurojust was also urged to send the list of priority countries to any new Presidency and

⁶⁰² In the Eurojust-US Agreement of 6 November 2006, no provision on liability is foreseen.

⁶⁰³ Cover Note in Council of the EU, *Opinion of Eurojust I on the practical implementation of Articles 26(2) last sentence, 26a(2) last sentence and 27a(1) of the revised Eurojust Decision*, 12479/10, Brussels, 22 July 2010.

to keep it informed regarding the concluded MoUs⁶⁰⁴ and to strengthen the link between the Eurojust's external action and that of the EU. The lack of direct control from the European Parliament, and the almost insignificant presence of the European Commission, makes Prof. Santiago affirm that the treaty-making proceeding really belonged to the former third pillar, i.e. the Council, and not Eurojust⁶⁰⁵. The Eurojust-European Commission MoU⁶⁰⁶ required the agency to regularly consult the European Commission on external policy issues and to take into account the Commission's priorities when deciding the list of third countries and organisations with which Eurojust should conclude new agreements. The same rationale applies to the Eurojust liaison magistrates as the Eurojust amended Decision proposed a Model Agreement that set forth the possibility for third countries to second their magistrates to Eurojust, while Eurojust Liaison Magistrates might be sent to third country territories⁶⁰⁷. The Model Agreement played a fundamental role in Eurojust's external relations as it was supposed to ensure the transfer of personal data with those countries that did not have a cooperation agreement due to the fact that they did not comply with the EU data protection standards⁶⁰⁸. Should the Council give a negative opinion on the deployment of liaison magistrates, Eurojust would be obliged to sign a cooperation agreement with the third country if liaison magistrates had already been deployed. The conclusion of the corresponding agreement was subjected to the approval of the Joint Supervisory Body, the President of Eurojust's College, and a favorable vote of the Council by qualified majority⁶⁰⁹. Hence, the majority of Eurojust's cooperation agreements have a clear binding nature – with the sole exception of the Eurojust-US agreement⁶¹⁰ – and their wording

⁶⁰⁴ Cover Note in Council of the EU, *Memorandum of Understanding between the European Commission and Eurojust*, 15962/11, Brussels, 24 October 2011, specifying that the Commission should not have access to 'operational data'.

⁶⁰⁵ Mirentxu Jordana Santiago, *op. cit.*, p. 77.

⁶⁰⁶ Eurojust-European Commission MoU, 20 July 2012. The MoU does not regulate the exchange of personal data. Another MoU was signed on 11 January 2010 on the management of financial transfers – María Esther Jordana Santiago, *op. cit.*, p. 196 –, but it is no longer available in the agency's official webpage.

⁶⁰⁷ Article 27a of the Eurojust amended Decision.

⁶⁰⁸ Council of the EU, 8862/13, Brussels, 26 April 2013, p. 10 ff.

⁶⁰⁹ Prior to the conclusion of these agreements, Eurojust could have received personal data directly from the third party '[...] in so far as this is necessary for the legitimate performance of its tasks' – Article 26a(5). On the contrary, it could transfer personal data, under the consent of the Member State transmitting the information, only when: this was necessary in individual cases for the purposes of preventing or combating criminal offences for which Eurojust is competent, and Eurojust would have concluded an agreement as referred to Article 26a(2) with the entity concerned.

⁶¹⁰ The majority of agreements foresee one or several norms on the implementation of the agreement except the EU-Iceland and the EU-Switzerland ones. Besides, the EU-Norway Agreement only provides for regular consultation on the implementation of the Agreement by virtue of its Article 7.

suggests that they have been concluded as international agreements⁶¹¹. Prof. Santiago notes that:

‘[...] this [proceeding] is still a requisition of the former third pillar’ since the European Commission was marginally consulted and the European Parliament not at all. The strict dependency Eurojust had with the Council confirms that these agreements could not be considered treaty under public international law [...] In the light of these aspects of the agreements concluded by Eurojust with third countries, it is not surprising that these agreements have often been described as undesirable and complicated to qualify, as they fall into a “grey area” of external action in the field of judicial cooperation which is reminiscent of the former third pillar and which does nothing to enhance the democratic legitimacy and legal quality of the AFSJ’⁶¹².

As a general rule, Eurojust’s cooperation agreements seem no different from those of Europol, for which they should be considered as executive agreements concluded on behalf of the EU without any real delegation taking place on the basis of the *Meroni* and subsequent rulings⁶¹³. As we explained *supra*, this would ensure that Eurojust’s cooperation agreements remain under public international law, which, on the contrary, covers those treaties that, although concluded in a simplified form, bind the underlying state or organisation. This explains why cooperation agreements have been suppressed in the new Eurojust Regulation in light of the new institutional balance settled by the Lisbon Treaty as far as the EU treaty-making power is concerned, as well as the 2012 Joint Statement on decentralised agencies. In Prof. Mitsilegas’ words, the Eurojust Regulation:

‘[...] essentially removes the competence of Eurojust to conclude international agreements with third States, although it provides for the possibility that Eurojust can conclude working arrangements to implement adequacy decisions or international agreements concluded between the European Union and a third State. The legal force and nature of these working arrangements is however unclear [...]’⁶¹⁴.

b) The transfer of personal data under the Eurojust Regulation

The Eurojust Regulation introduces relevant changes regarding the transfer of “operational personal data” among competent judicial authorities and confirms that Eurojust can maintain cooperation with the authorities of third countries and international organisations⁶¹⁵. Although the European Commission’s Proposal set forth the possibility for the College and the EDPS to authorise ‘sets of transfer[s]’ of personal data to third countries, following the prohibition to transfer information – including personal data – to third countries and organisations that have

⁶¹¹ See Andrea Ott, “EU regulatory agencies in EU external relations: Trapped in a legal minefield between European and international law”, *European Foreign Affairs Review*, Vol. 13, No. 4, 2008, pp. 515-540, p. 537.

⁶¹² Maria Esther Jordana Santiago, *op. cit.*, p. 189 (our own translation).

⁶¹³ See above.

⁶¹⁴ Council of the EU, 17188/1/13 REV 1, Brussels, 4 December 2013, p. 30.

⁶¹⁵ Article 52(1) of the Eurojust Regulation.

not concluded a cooperation agreement with Eurojust⁶¹⁶, this provision has not been included in the final text of the Eurojust Regulation. The transfer of operational personal data to third countries and international organisations is generally subjected to a series of requirements: its necessity according to Eurojust's tasks; the fact that the foreign authority is competent in law enforcement and criminal matters; the prior authorisation of the Member State that 'transmitted or made available' the data to Eurojust, unless it has already given previous authorisation, and the onward transfer of the data to other third parties after gaining Eurojust's authorisation⁶¹⁷. Thus, Eurojust is allowed to transfer operational personal data if there is⁶¹⁸:

- an adequacy decision, or an appropriate safeguard, or a specific derogation clause;
- a cooperation agreement concluded before 12 December 2019 according to Article 26a of the Eurojust amended Decision, or
- an international agreement between the EU and the third country or international organisation pursuant to Article 218 TFEU 'that provides for adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals'.

Despite initial uncertainties⁶¹⁹, the adequacy decision upon which Eurojust can rely will be adopted by the European Commission on the basis of Article 36 LED⁶²⁰. Second – and unlike Eurojust's suppressed cooperation agreements⁶²¹ – Eurojust is entitled to conclude 'legally binding instrument[s]' under the so-called 'appropriate safeguards' instrument⁶²² foreseen under Article 58(1)(a) of the Eurojust Regulation, which includes a positive assessment made by the own agency on the third party of which the EDPS is informed⁶²³. The former is of particular interest, as it allows Eurojust to conclude international administrative agreements on its own behalf, which requires due attention *vis-à-vis* Article 218 TFEU. If there is no adequacy decision or appropriate safeguard, the transfer of personal data can be channelled through derogation clauses⁶²⁴:

⁶¹⁶ Council of the EU, 8488/14, Brussels, 4 April 2014, p. 32.

⁶¹⁷ Article 56(1) of the Eurojust Regulation.

⁶¹⁸ Article 56(2) of the Eurojust Regulation.

⁶¹⁹ See the Joint Supervisory Body alleging the impossibility to rely on the DPD to adopt adequacy decisions for Eurojust in the Council of the EU, 17419/13, Brussels, 6 December 2013, p. 19.

⁶²⁰ Article 57 of the Eurojust Regulation.

⁶²¹ Article 56(2)(c) of the Eurojust Regulation.

⁶²² Article 58(1)(a) of the Eurojust Regulation.

⁶²³ Article 58(3) of the Eurojust Regulation.

⁶²⁴ Article 59 of the Eurojust Regulation.

- to protect the vital interests of the data subject or another person; to safeguard the legitimate interests of the data subject;
- for the prevention of an immediate and serious threat to the public security of a Member State or a third country, or
- in individual cases for the performance of Eurojust's tasks, unless it is determined that the fundamental rights and freedoms of the data subject concerned override the public interest in the transfer.

Finally, the Eurojust Regulation foresees that the transfer of personal data can be realised by virtue of an international agreement concluded between the EU and the third country or international organisation 'that provides for adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals' on the basis of Article 218 TFEU. This provision, together with the one suppressing Eurojust's cooperation agreements, confirms our assumption for which that the latter are international agreements unlawfully concluded on the EU behalf. On 19 November 2020, the European Commission issued a recommendation to the Council in order to receive the mandate to undertake negotiations with Algeria, Armenia, Bosnia and Herzegovina, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia, and Turkey and to conclude international agreements that would ensure the exchange of information between these countries and Eurojust⁶²⁵. Although generally satisfied by the negotiations, the EDPS⁶²⁶ complained about the lack of a substantive legal basis underpinning the negotiations and, once again, suggested inserting a reference to Article 16(2) TFEU. The EDPS revisited the necessity to assess if each third country meets the equivalent standards of protection as required by EU data protection law on a case-by-case basis and called for full cooperation among EU and foreign independent supervisory authorities in order to monitor the implementation of the Agreement. The Joint Supervisory Body, instead, complained about it while affirming that 'existing EU agreements with third States contain very limited data protection clauses and therefore, provide fewer guarantees than the existing Eurojust agreements with third countries'⁶²⁷.

⁶²⁵ Council of the EU, *Draft Council Decision authorising the opening of negotiations for Agreements between the European Union and Algeria, Argentina, Armenia, Bosnia and Herzegovina, Brazil, Colombia, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey on cooperation between the European Union Agency for Criminal Justice Cooperation (Eurojust) and the competent authorities for judicial cooperation in criminal matters of those third States - Adoption*, 5934/21, Brussels, 12 February 2021.

⁶²⁶ See the Opinion of the EDPS No. 10/2020 on *the negotiating mandate to conclude ten agreements allowing the exchange of data between Eurojust and the competent authorities for judicial cooperation in criminal matters in certain third countries*, Brussels, 17 December 2020.

⁶²⁷ See the Joint Supervisory Body alleging the impossibility to rely on the DPD to adopt adequacy decisions for Eurojust in the Council of the EU, 17419/13, Brussels, 6 December 2013, p. 19.

Consequently, in the case of Eurojust, the exchange of personal data from the EU to third countries and international organisations cannot be channelled through soft law or working arrangements, which is apparently in line with the EUDPR⁶²⁸ and the Europol Regulation⁶²⁹. The latter may be used only to ‘set out modalities to implement the agreements or adequacy decisions’⁶³⁰. This provision is consistent with the numerous MoUs concluded between Eurojust and third parties, including the Eurojust-Interpol MoU, that only concern non-operational information. Yet, the Eurojust Regulation makes safe two relevant instruments: firstly, the Council Common Position 2005/69/JHA on exchanging personal data with Interpol⁶³¹; and secondly, the Council Decision 2007/533/JHA on the establishment, operation, and use of the SIS II with Interpol⁶³². According to these instruments, the exchange of ‘operational’ personal data shall be realised only on a case-by-case basis, notwithstanding the existence, or not, of an underlying arrangement.

2.3. EBCG Agency’s external relations

The European Agency for the Management of Operational Cooperation at the External Borders’s (Frontex) was born following the substantial enlargement of the (then) European Community in 2004 as a coordinative agency, with no policymaking or implementing powers, and whose activity should have been strictly governed by the Member States’ instructions⁶³³. In this way, Member States could keep their prerogatives in patrolling external borders intact while relying on the operational support of the EU and, even more importantly, they temporarily avoided conferring on the EU an express competence regarding the management of external borders. As a result, Frontex’s main tasks consisted of⁶³⁴:

- first, performing risk analyses – also labelled as ‘intelligence product’ – directed at identifying threats and risks that could have undermined the integrated management of

⁶²⁸ See Article 37 LED.

⁶²⁹ See *supra*.

⁶³⁰ Article 56(3) of the Eurojust Regulation.

⁶³¹ Council Common Position 2005/69/JHA.

⁶³² See *supra*.

⁶³³ See Council Regulation (EC) 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, *OJ* L 349, 25.11.2004, pp. 1-11 (Frontex Regulation hereinafter) and Rut Bermejo Casado, “El proceso de institucionalización de la cooperación en la gestión operativa de las fronteras externas de la UE”, *Barcelona Centre for International Affairs*, No. 91, 2010, pp. 29-62, who underlines that, except from the United Kingdom, Member States actively contributed to the establishment of a common corps to patrol and control external borders in a coordinated manner, though in the intergovernmental framework.

⁶³⁴ Article 2 of the Frontex Regulation.

external borders⁶³⁵, which included information on the ‘flows, refusals and detections for illegal entry and facilitation at air, sea and land borders’⁶³⁶;

- second, training national border guards⁶³⁷;
- third, conducting research for the control and surveillance of external borders, for example, in the fields of modern technologies in border management such as biometrics and automated border crossing systems⁶³⁸, and
- fourth, supporting the Member States from an operational and technical point of view through the supply of technical equipment, the coordination of two or more Member States in case of cross-border issues concerning external borders, the deployment of experts to support competent national authorities, or the participation in operations regarding the return of illegal migrants.

Maintaining the Member States’ full sovereign powers turned out to be detrimental to the management of the external borders due to the lack of solidarity toward those subjected to high migration pressure⁶³⁹. Thus, the agency’s tasks were upgraded in 2007 with the provision of rapid border intervention teams through which the EU first showed off its physical presence at the external borders⁶⁴⁰. According to Prof. Mitsilegas:

⁶³⁵ Through its risk analysis unit, see recital (6) of the Frontex Regulation. Risk analysis reports are also relevant for the SCH-EVAL that was announced in the Council conclusions on the management of the external borders of the Member States of the European Union, 5 and 6 June 2008, and adopted with the Council Regulation (EU) 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen, *OJ L* 295, 6.11.2013, pp. 27-37. From the document of the Council of the EU, *Frontex Annual Risk Assessment 2012*, 10002/12, Brussels, 16 May 2012, p. 12, we understand that ‘threat’ is considered a force or pressure acting upon the external borders that is characterised by both its magnitude and likelihood; ‘vulnerability’, instead, is the capacity of a system to mitigate the threat, and ‘impact’ is the determined potential consequence of the threat.

⁶³⁶ See the Note from the Presidency in Council of the EU, *Preparation of the Schengen evaluation of the new Member States – Letter to the Frontex Agency: Request for risk analysis*, 12222/05, Brussels, 18 October 2005. Risk analysis concerned illegal border crossings, refusals of entry, asylum applications, detection of illegally stay, use of forged documents and detections of facilitators – see the Council of the EU, *New JHA working structures: Abolition of CIREFI and transfer of its activities to FRONTEX and the Working Party on Frontiers*, 6504/10, Brussels, 22 February 2010, p. 2.

⁶³⁷ Recital (7) Frontex Regulation.

⁶³⁸ Council of the EU, *Frontex Programme of Work 2008*, 17440/08, Brussels, 18 December 2008, p. 25.

⁶³⁹ See the document from the General Secretariat of the Council of the EU, – “Powers of the EU concerning migration by sea” – “Frontex training” – “Rescue of shipwrecked refugees” – “The dramatic situation of the migrants refused by Malta”, 11420/07, Brussels, 2 July 2007.

⁶⁴⁰ See Regulation (EC) 863/2007 of the European Parliament and of the Council of 11 July 2007 establishing a mechanism for the creation of Rapid border intervention teams and amending Council Regulation (EC) 2007/2004 as regards that mechanism and regulating the tasks and powers of guest officers, *OJ L* 199, 31.7.2007, pp. 30-39 (RABITs Regulation hereinafter). Rapid border intervention teams were made national staff extracted from the Rapid Pool, though the Member State concerned by ‘a mass influx of third country nationals’ was not obliged to put its national border guards at the disposal of a specific operation. Besides, the members of the team were required to wear ‘a blue armband with the insignia of the European Union and the Agency on their uniform’ according to Article 6(4) of the RABITs Regulation.

‘The RABITs Regulation has added detail on the legal framework of some aspects of FRONTEX operations and represents a clear shift from purely national to EU border control involving executive measures and coercive powers’⁶⁴¹.

The provision of rapid border intervention teams was a sign of the Member States’ progressive acceptance of Frontex’s power to initiate and coordinate operational activities in their territories⁶⁴². Yet, rapid border intervention teams were designed to provide *ad hoc* support for a limited period in case of emergency and according to a pre-defined operational plan⁶⁴³. The use of force should have been authorised by both the home Member State – that is the Member State of origin of the team members – and the host Member State, where the rapid border intervention teams would have been deployed in accordance with the national law of the latter. In addition, refusals of entry decisions were excluded from the agency’s competences and jealously retained within the Member State’s prerogatives⁶⁴⁴. However, such a “mixed cooperation” was subject to discussion from its very beginning, as the co-existence of national and EU bodies at the borders blurred the lines between national and EU responsibilities⁶⁴⁵. Provided that Member States remained responsible for the control of the external borders, any breach to the migrants’ human rights perpetrated by the agency’s staff could not be challenged⁶⁴⁶.

The European Commission proposed to increase the agency’s empowerment following the provision of an *ad hoc* legal basis inserted by the Lisbon Treaty. Notably the TFEU does not incorporate a specific rule regarding the agency, but a new competence on the integrated management system for external borders has been conferred to the EU⁶⁴⁷. Widespread negotiations that rapidly became political dialogues⁶⁴⁸ led to an amendment of Frontex’s

⁶⁴¹ Valsamis Mitsilegas, “Immigration Control in an Era of Globalization: Deflecting Foreigners, Weakening Citizens, Strengthening the State”, *Indiana Journal Global Legal Studies*, No. 3, Vol. 19, 2012, pp. 3-60, p. 34 ff. Also, in Pascouau’s point of view, the communitarisation of Frontex started with the implementation of the rapid border intervention teams – see Yves Pascouau, *La politique migratoire de l’Union Européenne. De Schengen à Lisbonne*, L.G.D.J., Paris, 2010, pp. 269-270.

⁶⁴² See the Council of the UE, *Frontex General Report 2007*, 17441/08, Brussels, 18 December 2008, p. 18.

⁶⁴³ Recital (7) of the RABITs Regulation.

⁶⁴⁴ Article 6(10) of the RABITs Regulation.

⁶⁴⁵ See Valsamis Mitsilegas, *loc. cit.*

⁶⁴⁶ See, for example, the Council of the EU, “*Media reports of human rights violations by the European border management agency Frontex*”, 16040/09, Brussels, 16 November 2009.

⁶⁴⁷ Article 77(2)(d) TFEU. See the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Report on the evaluation and future development of the FRONTEX Agency, COM(2008) 67 final, Brussels, 13.02.2008. The Proposal to insert a definition of integrated border management in the Schengen Borders Code was discarded – see the Council of the EU, *Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No 207/204 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)*, 968/10, Brussels, 1 May 2010, p. 2.

⁶⁴⁸ Council of the EU, *Strengthening the European external borders agency Frontex - Political agreement between Council and Parliament*, 11916/11, Brussels, 23 June 2011.

mandate in 2011⁶⁴⁹ and although the agency still lacked decision-making powers, it was mandated to facilitate and render more effective the application of existing and future EU measures relating to the Schengen Borders Code⁶⁵⁰. All in all, Frontex's tasks were enhanced in order to provide technical equipment for external borders and to deploy joint operations, pilot projects, and rapid interventions⁶⁵¹ that stemmed from a unique European border guard force⁶⁵² drawn from a common pool⁶⁵³. Specifically, joint operations and pilot projects could have been proposed by the Member States or Frontex itself; yet, if proposing a project, Frontex should have counted on the host Member State's willingness to intervene.

Thanks to the European Parliament's presence in the ordinary legislative procedure, the Frontex amended Regulation was replete with EU fundamental rights norms. The Executive Director was empowered to suspend or terminate joint operations and pilot projects in case breaches of fundamental rights or international protection obligations 'of a serious nature' were

⁶⁴⁹ Regulation (EU) 1168/2011 of the European Parliament and of the Council of 25 October 2011 amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, *OJ L* 304, 22.11.2011, pp. 1-17 (Frontex amended Regulation hereunder). It can be noted that the new Regulation was adopted based on Articles 74 and 77(2)(b) and (d) TFEU though the European Commission proposed based on Articles 74 and 77(1)(b) and (c) TFEU.

⁶⁵⁰ Article 1 of the Frontex amended Regulation.

⁶⁵¹ For which purposes a joint operations unit has been established according to Articles 3 and 3a of the Frontex amended Regulation.

⁶⁵² Article 3b of the Frontex amended Regulation was largely discussed during the negotiations since the delegations did not want to be obliged to submit their own border guards to the Frontex pool. An agreement was found in the trialogue for which: 'The contribution by Member States as regards their border guards to specific joint operations and pilot projects for the following year shall be planned on the basis of annual bilateral negotiations and agreements between the Agency and Member States. In accordance with those agreements, Member States shall make the border guards available for deployment at the request of the Agency, unless they are faced with an exceptional situation substantially affecting the discharge of national tasks. Such a request shall be made at least 45 days before the intended deployment. The autonomy of the home Member State in relation to the selection of staff and the duration of their deployment shall remain unaffected'. Notably, and although the United Kingdom could not opt-in the Regulation, it wanted contribute to the funding of the agency and, consequently, it was invited to participate in Frontex activities thanks to the conclusion of bilateral arrangements with the Member States – see the Council of the EU, *Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEx)-Analysis of the final compromise text with the view to agreement*, 12341/1, Brussels, 5 July 2011, p. 32.

⁶⁵³ Articles 3b and 3c of the Frontex amended Regulation and the Council of the EU, *Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEx)*, 10594/11, Brussels, 26 May 2011. With the rapid border intervention teams, Frontex started to conclude bilateral arrangements with the Member States to deploy "Frontex Joint Support Teams" also in case of non-emergency situations – see the Council of the EU, *Commission Staff working document Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEx)*, 6898/10 ADD 1, Brussels, 1 March 2010, p. 13. See also Article 7 of the Frontex amended Regulation after huge negotiations where Member States' delegations tried to have the equipment financed by Frontex a hundred percent finally opted for the co-ownership of the equipment.

detected, or if the Executive Director believed that they were likely to continue occurring⁶⁵⁴. Moreover, the agency adopted a code of conduct to facilitate the return of illegal migrants ‘in a humane manner and with full respect for: fundamental rights, principles of human dignity, prohibition of torture and of inhuman or degrading treatment or punishment, the right to liberty and security and the rights to the protection of personal data and non-discrimination’⁶⁵⁵. Frontex’s contribution in joint return operations was subjected to a monitoring mechanism ‘on the basis of objective and transparent criteria [that must have covered] the whole joint return operation’⁶⁵⁶. Finally, Frontex was empowered to coordinate joint return operations and to cooperate with the competent authorities of third countries to identify best practices on the acquisition of travel documents and the return of illegally present third-country nationals, it also developed common core curricula for the training of border guards⁶⁵⁷.

The agency faced its major transformation after the humanitarian crisis of 2015 when the “hotspot approach”⁶⁵⁸ was experimented with for the first time⁶⁵⁹. The “hotspot approach” represented a crucial laboratory for procedures and approaches concerning the identification, registration and fingerprinting of third country nationals, as well as for the provision of information on the asylum process input in the Eurodac by national competent authorities. After the individuals were screened, each agency could support domestic authorities according to their specific mandate: Frontex was in charge of returning illegal migrants; the EUAA submitted international protection requests or draft relocation schemes⁶⁶⁰, while Europol and Eurojust assisted the Member States in the investigation of organised criminal networks with secondary-line checks. According to Commissioner Dimitris Avramopoulos:

⁶⁵⁴ Article 3(1) *in fine* Frontex amended Regulation.

⁶⁵⁵ Article 9 of the Frontex amended Regulation. Frontex liabilities in returning irregular migrants *vis-à-vis* the principle of non-refoulement has been extensively analysed by Roberta Mangianu, *Frontex and Non-Refoulement. The International Responsibility of the EU*, Cambridge, Cambridge Studies in European Law and Policy, 2016.

⁶⁵⁶ Article 9(1b) of the Frontex amended Regulation.

⁶⁵⁷ Article 4(8) of the Frontex amended Regulation.

⁶⁵⁸ See the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, a European Agenda on Migration, COM(2015) 240 final, Brussels, 13.5.2015.

⁶⁵⁹ The “hotspot approach” put EU freedom, security, and justice’s agencies on the frontline in order to support Member States facing disproportionate migratory pressures made of “mixed” flows as it was the case of Italy and Greece. Its opportunity is evaluated on the basis of risk analyses assessment conducted by the EBCG Agency and the (now) EUAA so that the European Commission may advance its own proposal to establish a Hotspot area or the Member States itself could have required it if affected by migratory pressure. In any case, the establishment of a hotspot area must last only in an emergency situation.

⁶⁶⁰ See *infra*.

‘The result of combining information, operational support and capacity building activities from all relevant EU Agencies should amplify the impact of assistance, which would be greater and more visible than when provided by EU Agencies separated’⁶⁶¹.

Having been replaced by the EBCG Agency in 2016⁶⁶², Frontex’s mandate was expanded so as to cover a (vast) definition of integrated border management⁶⁶³ which, arguably, enhanced the Union’s intervention beyond its empowerment⁶⁶⁴. Under the new Regulation, the implementation of the EU integrated border management system was no longer the sole responsibility of the Member States, but rather it was shared between the States and the EBCG⁶⁶⁵. That definition confirmed that the agency’s mandate concerned both:

- the managing of migratory flows to return illegal migrants within a return operation or a return intervention by acquiring the travel documents of returnees⁶⁶⁶, and
- the protection of the EU external borders to combat serious crime with a cross-border dimension— such as migrant smuggling, trafficking in human beings and terrorism – so as to ensure a high level of internal security in close cooperation with Europol⁶⁶⁷.

Notably, both fields of competences have progressively shifted the agency’s operational activity toward the detection of false documents and identity fraud which granted the agency access to the iFADO database⁶⁶⁸. In addition, a horizontal expert group on document fraud was

⁶⁶¹ See the Council of the EU, –“Hotspot” approach -FRONTEX support to return of irregular migrants –“Sage countries of origin”, 10962/15, Brussels, 15 July 2015, p. 9.

⁶⁶² Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No. 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC, *OJL* 251, 16.9.2016, pp. 1-76 (2016 EBCG Agency Regulation hereinafter).

⁶⁶³ Article 4 of the 2016 EBCG Agency Regulation.

⁶⁶⁴ José Alejandro del Valle Gálvez, 2016, *op. cit.*, pp. 759-777, p. 768 ff., calls for the provision of new legal bases in the founding Treaties to legitimise the ‘external border policy’ the EU has been promoting since the humanitarian crisis of 2015.

⁶⁶⁵ Article 5 of the 2016 EBCG Agency Regulation.

⁶⁶⁶ See recital (32) of the 2016 EBCG Agency Regulation, though Member States still keep the prerogative of deciding the merits of a return decision. It is really welcomed the insertion of specific provisions on minors in recitals (37)-(38).

⁶⁶⁷ Recital (19) of the 2016 EBCG Agency Regulation.

⁶⁶⁸ See the Council of the EU, *Use of images of the iFADO database for Frontex Quick Check Cards*, 7819/16, Brussels, 28 April 2016, that recalls the Joint Action 98/700/JHA of 3 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union concerning the setting up of a European Image Archiving System (FADO), *OJL* 333, 9.12.1998, pp. 4-7, repealed by Regulation (EU) 2020/493. The 2019 EBCG Agency Regulation also incorporates the regime on the FADO system – recital (95) and Article 10(ae) of the 2019 EBCG Agency Regulation according to which: ‘It is therefore intended that the Agency take over the administration and the operational and technical management of the FADO system from the General Secretariat of the Council as soon as the European Parliament and the Council have adopted the relevant legal act on the FADO system replacing Joint Action 98/700/JHA’. Confront the Council of the EU, *Frontex’ request of access to Expert FADO and to Expert FADO test environment*, 5669/21, Brussels, 28 January 2021.

set up in cooperation with Europol⁶⁶⁹. The combat of identity fraud was indeed one of the new features inserted in the concept of integrated border management set down in the 2019 EBCG Agency Regulation⁶⁷⁰. Also, the 2016 reform was an important step toward the enhancement of the protection of fundamental rights within the agency's activities⁶⁷¹, though it was probably not sufficient given the recent allegations regarding the agency pushing back against asylum seekers at the Member States' external borders⁶⁷².

In 2019 the EBCG Agency was empowered with a permanent standing staff of 10,000 operational staff members with executive powers⁶⁷³. The agency's corps is deployed in the Member States to regularly monitor the management of the external borders and to assist in return operations⁶⁷⁴. Liaison officers are in charge of, for example: supporting the collection of information required for the monitoring of illegal immigration and risk analyses; carrying out vulnerability assessments and preparing a report for that purpose; facilitating communication between the Member State concerned and the agency; sharing relevant information from the agency with the Member State concerned, including information about ongoing operations, and monitoring the measures taken by the Member State with regard to returns, and supporting the collection of information required by the agency to carry out its activities⁶⁷⁵.

⁶⁶⁹ Council of the EU, *Joint Europol – Frontex concept note for a possible way forward with regard to the establishment of the horizontal expert group on document fraud*, 10910/17, Brussels, 7 July 2017. The *Situational Overview 2017 prepared by Europol and Frontex as input for the Document Fraud*, 15051/17, Brussels, 4 December 2017, highlights how document frauds become an issue not only to cross external borders but also to refrain secondary movement within the Schengen area.

⁶⁷⁰ 2019 EBCG Agency Regulation. Council of the EU, *Frontex draft Programming Document 2019 - 2021*, 5247/18, Brussels, 30 January 2018, p. 17.

⁶⁷¹ Article 109 of the 2019 EBCG Agency Regulation confirms the existence of a fundamental rights officer as established in 2016.

⁶⁷² Which caused the resignation of the Executive Director according to “Mis en cause par l'OLAF et des enquêtes de presse sur les pratiques de refoulement, Fabrice Leggeri quitte la tête de l'agence Frontex”, *Bulletin Quotidien Europe*, No. 12942, 30.4.2022. See the project Not on our border watch launched by the law firm Prakken d'Oliviera Human Rights Lawyers, the Dutch Council for Refugees, the campaign agency BKB and Sea Watch Legal Aid, together with the support of several European NGOs, available at www.notonourborderwatch.com.

⁶⁷³ Articles 5(2) and 54 ff. of the 2019 EBCG Agency Regulation. The EBCG standing corps should be composed of three categories of operational staff: first, staff members employed by the EBCG Agency; second, staff mandatorily seconded to the agency by the Member States for long duration, and third, staff mandatorily provided by Member States for short-term deployment – see recital (58) of the 2019 EBCG Agency Regulation. The operational staff is deployed as members of the teams and has the necessary powers to carry out border control and return tasks, including the tasks requiring executive powers, set out in relevant national law or in the 2019 EBCG Agency Regulation – see recital (59) of the 2019 EBCG Agency Regulation.

⁶⁷⁴ Article 31 of the 2019 EBCG Agency Regulation.

⁶⁷⁵ Article 31(3) of the 2019 EBCG Agency Regulation.

Liaison officers and reports on national situations⁶⁷⁶ enable the agency to create vulnerability assessments⁶⁷⁷ that detect weaknesses⁶⁷⁸ in the Member States' border management systems. If a vulnerability is detected, the Executive Director might urge the Member States to adopt a contingency plan that, in case of non-compliance, would be referred to the Management Board. In this case, the Member State concerned is obliged to address the vulnerability under the monitoring and instructions of the Executive Director⁶⁷⁹: 'If the Member State does not implement the measures within the time limit provided for in that decision, the management board shall notify the Council and the Commission and further action may be taken in accordance with Article 42'⁶⁸⁰. That is: control at the internal borders can be re-established by the Member States according to Article 29 of the Schengen Borders Code⁶⁸¹ to prevent secondary movements⁶⁸². Similarly, a unified, rapid, and effective response is delivered at Union level if the Council detects risks that jeopardise the functioning of the Schengen area, either because a Member State does not take the necessary measures in line with a vulnerability assessment, or because a Member State facing specific and disproportionate challenges at the external borders has not requested sufficient support from the agency, or is not implementing such support. If this is the case, the EBCG Agency must implement the Council's decision that can include:

- organising and coordinating rapid border intervention teams and the deployment of European border and coast guard teams from the rapid reaction pool, and additional European border and coast guard teams as appropriate;
- deploying European border and coast guard teams as part of the migration management support teams at hotspot areas;
- coordinating the activities of one or more Member States and third countries at the external borders, including joint operations with neighbouring third countries; deploying technical equipment, and organising return interventions.

⁶⁷⁶ Article 12(4)(a) of the EBCG Agency Regulation and the Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosir), *OJ L* 295, 6.11.2013, p. 11-26 (EUORSUR Regulation hereinafter).

⁶⁷⁷ Article 13 of the 2019 EBCG Agency Regulation.

⁶⁷⁸ Vulnerability assessments are directed at assessing the capacity and readiness of the Member States to face challenges at their external borders and to contribute to the standing corps and technical equipment pool – recital (43) and Article 32 of the 2019 EBCG Agency Regulation – complementing the SCH-EVAL mechanism – recital (45) and Article 33 of the 2019 EBCG Agency Regulation.

⁶⁷⁹ Article 34 ff. of the 2019 EBCG Agency Regulation set forth that on this basis, the EBCG Agency could have assigned an impact level to each external border section as low, medium, or high impact.

⁶⁸⁰ Article 32(10) of the 2019 EBCG Agency Regulation.

⁶⁸¹ Recital (57) of the 2019 EBCG Agency Regulation.

⁶⁸² Article 9(2) of the 2019 EBCG Agency Regulation.

If, once notified, a Member State affected by vulnerabilities does not attend to the Council's decision, then, the latter may decide to re-introduce controls on internal borders⁶⁸³. Rapid border intervention teams aside⁶⁸⁴, patrol deployments rely on the European Border and Coast Guard teams⁶⁸⁵ that are deployable for joint operations⁶⁸⁶ in the Member States or third countries' territories, and these include:

- border management teams, that can be deployed in the Member States for 'the appropriate duration' to 'assist' Member States in facilitating the crossing of external borders⁶⁸⁷;
- migration management teams that will participate in the hotspot mechanism⁶⁸⁸ together with the other freedom, security, and justice agencies involved⁶⁸⁹, and
- return teams, that can charter aircraft, schedule flights⁶⁹⁰, and propose the coordination or organisation of return operations⁶⁹¹.

Although not empowered to initiate criminal investigations, the EBCG Agency can organise and coordinate joint operations for one or more Member States under their, or the Executive Director's, recommendation⁶⁹². These teams are coordinated by an officer of the agency that is in charge, *inter alia*, of monitoring the implementation of the previously agreed operational plan⁶⁹³, and also in cases of 'multipurpose operations' where both joint operations and rapid

⁶⁸³ Article 19 of the 2019 EBCG Agency Regulation and Article 29 of the Schengen Borders Code.

⁶⁸⁴ Article 39 of the 2019 EBCG Agency Regulation. Rapid borders intervention teams are deployed in case of 'specific and disproportionate challenge at the external border' and can be activated under the own agency's initiative with the agreement of the State concerned or by the own States.

⁶⁸⁵ Article 20 of the 2019 EBCG Agency Regulation.

⁶⁸⁶ Articles 37 and 38 of the 2019 EBCG Agency Regulation.

⁶⁸⁷ Article 10(1)(ag) of the 2019 EBCG Agency Regulation.

⁶⁸⁸ The implementation of hotspots instead is reserved to situation of 'specific and disproportionate migratory challenges at particular areas of its external borders characterised by large, inward, mixed migratory flows, the Member States should be able to rely on increased technical and operational reinforcements' according to recital (50) of the 2019 EBCG Agency Regulation.

⁶⁸⁹ Recital (25) ff. and Article 18 of the 2019 EBCG Agency Regulation.

⁶⁹⁰ In these terms, the EBCG Agency supports the readmission operations within the EU-Turkey Statement from the Greek hotspots according to the Council of the EU, *Frontex Evaluation Report on return operations - 2nd semester of 2019*, 8920/20, Brussels, 18 June 2020, p. 4.

⁶⁹¹ Article 33 of the 2019 EBCG Agency Regulation. Upon request, the EBCG Agency may deploy return interventions teams to a requesting Member States and organise the return operations from its territory, similarly the EBCG Agency may intervene through rapid border intervention teams when 'a Member State is facing specific and disproportionate challenges when implementing its obligation to return third-country nationals who are the subject of return decisions issued by a Member State'.

⁶⁹² Article 41 of the 2019 EBCG Agency Regulation.

⁶⁹³ Article 22 of the 2019 EBCG Agency Regulation.

border intervention teams collaborate⁶⁹⁴. Although the Member State concerned my refuse to implement one of these actions, it cannot put the functioning of the Schengen area at risk⁶⁹⁵.

2.3.1. The processing of personal data by the EBCG Agency

From the very beginning the EBCG Agency planned an integrated platform for the Member States, creating a network to exchange information to control and monitor/supervise the southern maritime borders through the implementation of National Coordination Centres⁶⁹⁶ that were connected via the European border-surveillance system (EUROSUR)⁶⁹⁷. It also developed a European patrols network, and it developed a Global Monitoring for Environment and Security to build pre-frontier pictures. In these terms, the EBCG Agency Situation Centre became a “hub” for the exchange of real-time operational information developed by an intelligence-led information system. Additionally, when the EBCG Agency started its operational activity, other networks for the exchange of risk analysis information existed, including:

- the Information and Co-ordination Network for Member States’ Migration Management Services, and
- the meetings held in the Centre for Information, Discussion and Exchange on the Crossing of Frontiers and Immigration⁶⁹⁸.

While the former enabled the exchange of information on visa and document forgeries and on best practices to combat counterfeiting and forgeries, as well as for establishing the identity of third country nationals and obtaining travel documents for return purposes, the latter improved the mechanism through which false and falsified travel documents could be detected and on ways of improving return practices. The European Commission decided to centralise the exchange of operational information on illegal immigrants in the EBCG Agency’s hands⁶⁹⁹,

⁶⁹⁴ Article 15(5) of the 2019 EBCG Agency Regulation: ‘The objectives of a joint operation or rapid border intervention may be achieved as part of a multipurpose operation. Such operations may involve coast guard functions and the prevention of cross-border crime, including the fight against migrant smuggling or trafficking in human beings, and migration management, including identification, registration, debriefing and return’.

⁶⁹⁵ Article 42 of the 2019 EBCG Agency Regulation.

⁶⁹⁶ See the Council of the EU, *Frontex feasibility study on Mediterranean Coastal Patrols Network – MEDSEA*, 12049/06, Brussels, 20 November 2006.

⁶⁹⁷ The EUROSUR also processes personal data pictures concerning ship identification numbers in the frame of situational picture and common pre-frontier intelligence – see Article 13 of the EUROSUR Regulation.

⁶⁹⁸ Council of the EU, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Report on the evaluation and future development of the FRONTEX Agency*, 6664/08, Brussels, 19 February 2008, p. 5 ff.

⁶⁹⁹ Council of the EU, *Commission Staff Working Documents accompanying document to the Communication from the Commission to the European Parliament the Council, the European Economic and Social Committee of the Regions Report on the evaluation and future development of the FRONTEX Agency Impact Assessment*,

but no provision on the protection of personal data was foreseen in its first regulation⁷⁰⁰ as the agency was not supposed to process personal data.

With the 2011 reform, the EBCG Agency took charge of ‘the development of a common information sharing environment, including interoperability of systems’⁷⁰¹. Provided that rapid border intervention teams were granted access to the host Member State’s national and European databases required for border checks and surveillance, the 2011 Proposal launched a crucial debate on the need and limits within which the EBCG Agency should have been allowed to process personal data⁷⁰². Specifically, the host Member State was expected to inform the agency of the systems that could be consulted if a rapid border intervention team was deployed in its territory, and the agency itself could make the information available to all Member States participating in such a mission⁷⁰³. Even though the European Commission proposed not to enable the agency to process personal data, both the delegations⁷⁰⁴ and the agency itself⁷⁰⁵ pressured the co-legislators to finally negotiate data protection provisions so that new references to the DPD were inserted in the RABITs Regulation⁷⁰⁶. In the Regulation, the agency was empowered to develop and operate information systems for the ‘[...] swift and reliable exchanges of information regarding emerging risks at the external borders, including the Information and Coordination Network established by Decision 2005/267/EC’⁷⁰⁷. Special emphasis was put on the exchange of classified information, including personal data⁷⁰⁸ that also fell within the scope of the ECDPR, rather than merely concerning the processing of ‘administrative data’⁷⁰⁹. From the inter-institutional debates, we infer that administrative

6664/08 ADD 1, Brussels, 19 February 2008, p. 13. The Centre for information, discussion and exchange on the crossing of frontiers and immigration was transferred to Frontex and to the Working Party on Frontiers in 2010; the latter, specifically, was in charge of presenting reports on Immigration liaison officers – see the Council of the EU, 6504/10, Brussels, 22 February 2010.

⁷⁰⁰ See Article 11 of the Frontex Regulation.

⁷⁰¹ See Article 1(3) of the Frontex amended Regulation.

⁷⁰² Council of the EU, *Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) - Personal data related issues*, 13466/10, Brussels, 14 September 2010.

⁷⁰³ Article 6(8) of the RABITs Regulation.

⁷⁰⁴ Council of the EU, *Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) – the necessity for FRONTEX to process personal data*, 15337/10, Brussels, 28 October 2010.

⁷⁰⁵ *Ibidem*.

⁷⁰⁶ Recital (19) of the RABITs Regulation.

⁷⁰⁷ Article 11 of the Frontex amended Regulation.

⁷⁰⁸ The United Kingdom and Ireland were granted a special status provided that they could not participate in the Regulation according to Article 11 of the Frontex amended Regulation.

⁷⁰⁹ Article 11a of the Frontex amended Regulation.

personal data referred to, for example, data processed for recruitment, for the management of the agency's staff in the rapid pool, for the issuing of accreditation documents to guest officers and rapid team members, or for the organisation of training and meetings. Operational data, instead, would be processed by Frontex as part of its operational tasks in the context of joint return operations, for the purposes of providing medical care, and for the safety and security of the operation. Yet there was still 'practical difficulty to clearly distinguish between FRONTEX's operational and non-operational activities and, more specifically, the cases in which the processing of personal data would take place for *purely administrative* or *purely operational purposes*'⁷¹⁰.

Provided that the Frontex amended Regulation shifted its mandate further toward the fight against crime rather than the control of migratory flows⁷¹¹, establishing which data protection regime should have been applicable to the agency's activities became the major challenge as far as its operational tasks were concerned. The EBCG Agency processed personal data in order to:

- implement the early warning mechanism;
- facilitate investigations and prosecutions on cross-border crimes and trafficking in human beings;
- recognise and detect false documents and the people using them⁷¹²;
- maintain situational pictures, and
- transmit information during joint sea operations.

As part of its joint operations, pilot projects, and rapid interventions the agency proactively contributed to returning illegal migrants 'without prejudice to the competence of the Member States to collect personal data'⁷¹³. While the organising Member State was in charge of contacting third country authorities, the EBCG Agency should have passed the passenger lists to airlines⁷¹⁴ in which cases personal data should have been retained for a maximum of ten days

⁷¹⁰ Council of the EU, *Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)*, 10127/10, Brussels, 25 May 2010, p. 7. Although the EDPS appreciated the provision of a Data Protection Officer, it also highlighted that the Regulation should have foreseen norms on data subjective rights – p. 8 ff.

⁷¹¹ Council of the EU, 15337/10, Brussels, 28 October 2010, p. 2.

⁷¹² For which purpose, Frontex should have implemented a centre of expertise for the detection of forged documents – see the Council of the EU, *Frontex Programme of Work 2011*, 5691/11, Brussels, 25 January 2011, p. 49.

⁷¹³ Article 11c of the Frontex amended Regulation.

⁷¹⁴ Opinion of the EDPS on a notification for Prior Checking received from the Data Protection Officer of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) concerning the "Collection of names and certain other relevant data of

after the end of the operation⁷¹⁵. In this layer, the EBCG Agency supporting activities consisted of, *inter alia*, procuring travel documents to execute the repatriation and, consequently, identification of people to be expelled through a pre-screening evaluation that tried to assess the migrants' nationality⁷¹⁶. This specific point gained the attention of the EDPS⁷¹⁷ as it enabled both the agency and the organising Member State to transmit information, including personal data⁷¹⁸, to third countries in order to execute the return of illegal migrants⁷¹⁹. Notably, as part of the EBCG Agency's rescue operations the agency has been processing personal data as it is empowered to screen third country nationals after disembarkation⁷²⁰. The migrants' data could have been combined with data on suspicious and/or confirmed methods of transportation used for the unauthorised crossing of external borders⁷²¹. The agency publicly reassured that the migrants' personal data would not be used to create risk analyses – i.e., profiling –, and only the data of the facilitators and/or members of criminal networks would be used. According to the EBCG Agency:

‘In order to make accurate identifying “targets” common characters like age, gender and nationality must be used in Frontex analyses. This targeting would need to include certain behavioural data such as lifestyles, movements, places frequently visited characters, traits, economic situations and roles in the criminal network. All this data is necessary to the

returnees for joint return operations (JRO)”, Brussels, 26 April 2010. The EDPS recommended to the agency to assess whether the airline at stake was subjected or not to DPD and, in the latter hypothesis, to take appropriate measures to comply with it, and also to provide the migrant/data subject the necessary procedures to grant his/her subjective rights.

⁷¹⁵ Article 11b of the Frontex amended Regulation. This possibility was inserted following a Presidency's Proposal that was not supported by the European Commission as you can see in the document on the Council of the EU, *Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)*, 10538/10, Brussels, 9 June 2010, p. 2.

⁷¹⁶ Council of the EU, *Draft conclusions on the improvement of cooperation between Member States, the Commission and FRONTEX with regard to expulsion*, 8329/07, Brussels, 13 April 2007.

⁷¹⁷ See Article 9 of the Frontex Regulation.

⁷¹⁸ Article 5(a) of the ECDPR enabled the transfer to third countries for ‘or performance of a task carried out in the public interest’.

⁷¹⁹ See also the Council of the EU, *Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)*, 17451/10, Brussels, 13 December 2010, differentiating the processing of personal data per operational activity. It may be added that the Visa Code has inserted new provisions on the monitoring of third countries' cooperation in the readmission field, which is also based on the collection of data but has a policy-making objective and not an operational one – see recital (13) for example.

⁷²⁰ Council of the EU, *Frontex Annual Report on the implementation on the EU Regulation 656/2014 of the European Parliament and of the Council of 15 May 2014 establishing rules for the surveillance of the external borders*, 11162/15, Brussels, 24 June 2015, p. 7.

⁷²¹ Within the EU borders, Lithuania, Poland, and Latvia lay at the core of the European Commission's Action Plan 2021-2025 against migrant smuggling and trafficking networks for which the Ylva Johansson proposed an intervention of Frontex in which case Europol's cooperation is also foreseeable – see the “Réseaux de passeurs, la Commission veut sanctionner les pays tiers qui instrumentalisent la migration”, *Bulletin Quotidien Europe*, No. 12801, 30.9.2021, and the “Europol peine à aider les États membres dans leur lutte contre les passeurs, selon la Cour des comptes européenne”, *Bulletin Quotidien Europe*, No. 12802, 1.10.2021.

identification of smugglers trafficking human beings and other related cross-border crime⁷²².

The agency could process personal data concerning persons who were suspected, on reasonable grounds, by the competent authorities of the Member States of involvement in cross-border criminal activities, in facilitating illegal migration activities, or in human trafficking activities⁷²³. It could, on a case-by-case basis⁷²⁴, transmitted the data to Europol and other law enforcement agencies, or it could ‘depersonalised’ it and used it for the elaboration of its risk analyses⁷²⁵. The Frontex amended Regulation specified that only the Member States were responsible for the eventual investigations stemming from the processing activity and that any onward transmission was prohibited. The possibility for the agency to process personal data related to the fight against criminal networks organising illegal immigration was explored after the European Commission’s proposal on the condition that such processing of personal data by Frontex was lawful, necessary, and proportionate in relation to its tasks⁷²⁶. Yet, the debate was postponed since the ECDPR applied to Frontex’s operational activities⁷²⁷ – except in case of the realisation of operations commanded by the host Member States, for which national law would have been applicable –, but it did not foresee any disposition for the processing of personal data as part of PJCCM.

The integrated border management concept inserted by the 2016 EBCG Regulation included within the agency’s mandate the use of state-of-the-art technology and large-scale information

⁷²² See for example the PeDRA Pilot exercise concerning the processing of personal data collected by Frontex during interviews conducted in Italy, Spain, and Greece, and then shared with Europol as described in the Council of the EU, *Frontex Annual Activity Report 2016*, 11442/17, Brussels, 20 July 2017, p. 29.

⁷²³ Council Directive 2002/90/EC of 28 November 2002 defining the facilitation of unauthorised entry, transit and residence, *OJ L* 328, 5.12.2002, pp. 17-18.

⁷²⁴ Article 11c(3)(a) of the Frontex amended Regulation.

⁷²⁵ Article 11c(1) of the Frontex amended Regulation. The deadline for its storage should have not exceeded three months after the date of collection.

⁷²⁶ Council of the EU, *Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEx)*, 6898/10, Brussels, 1 March 2010, p. 4. The Proposal set forth new provisions on: organisational aspects of joint operations and pilot projects; the composition of Frontex Joint Support Teams; a new provision on the processing of personal data according to the ECDPR; security measures on the protection of classified and non-classified sensitive information; the agreement of a headquarters for the agency.

⁷²⁷ Interestingly, the use of personal data for risk analysis purposes was justified by Frontex on the basis of the elaboration of a ‘target’ useful for border control activities, but it was considered suspicious by the delegations that finally found an agreement during the trialogue meetings. See the Council of the EU: 15337/10, Brussels, 28 October 2010, p. 7, and *Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEx)*, 8861/11, Brussels, 13 April 2021, p. 4.

systems, to which the EBCG Agency has been gaining increasing access⁷²⁸. Specifically, the agency can⁷²⁹:

- support the development of technical standards for equipment, especially for tactical-level command, control, and communication, as well as technical surveillance to ensure interoperability at Union and national level;
- develop and operate, in accordance with the ECDPR and the DPDFD, information systems that enable swift and reliable exchanges of information regarding emerging risks in the management of the external borders, illegal immigration and return, in close cooperation with the Commission, Union bodies, offices and agencies as well as the European migration network, and
- provide the necessary assistance for the development and operation of the EUROSUR and, as appropriate, for the development of a common information-sharing environment, including interoperability of systems, in particular by developing, maintaining, and coordinating the EUROSUR framework.

The agency's capability in the information field was last enhanced with the 2019 EBCG Agency Regulation⁷³⁰ that imposes on the Member States the obligation to share their information with the agency, except if this affects their internal security interests⁷³¹. Also, Member States' authorities are required to lawfully enter accurate and up-to-date information in European databases⁷³² to support the EBCG Agency in the creation of general and specific

⁷²⁸ Council of the EU, *Non-paper by Frontex on its access to central EU systems for borders and security*, 15174/17, Brussels, 1 December 2017.

⁷²⁹ Article 8 of the 2019 EBCG Agency Regulation.

⁷³⁰ Article 10(1) letters (y)-(ac) of the 2019 EBCG Agency Regulation foresees that the EBCG Agency can: develop technical standards for information exchange; support the development of technical standards for equipment in the area of border control and return, including for the interconnection of systems and networks, and support, as appropriate, the development of common minimum standards for external border surveillance, in line with the respective competences of the Member States and of the Commission; establish and maintain the communication network referred to in Article 14 of the same Regulation; develop and operate, in accordance with the EUDPR, information systems that enable swift and reliable exchanges of information regarding emerging risks in the management of the external borders, illegal immigration and return, in close cooperation with the European Commission, Union bodies, offices and agencies as well as the European migration network, and provide the necessary assistance for the development of a common information-sharing environment, including interoperability of systems, as appropriate.

⁷³¹ Recital (25) and Articles 11 and 12 of the 2019 EBCG Agency Regulation. Article 12(3) also provides for the adoption of measures facilitating the exchange of information with Ireland and the United Kingdom. The Member States' collaboration should contribute relevant data necessary for the activities carried out by the agency, including for the purposes of situational awareness, risk analysis, vulnerability assessments and integrated planning.

⁷³² Recital (17) of the EBCG Agency Regulation, and recital (26) of the 2019 EBCG Agency Regulation.

risk analyses⁷³³. Indeed, the EBCG Agency's teams are granted access to large-scale IT systems in the execution of their tasks. Article 82(19) of the 2019 EBCG Agency Regulation states:

‘[...] the host Member State shall authorise members of the teams to consult Union databases, the consultation of which is necessary for fulfilling operational aims specified in the operational plan on border checks, border surveillance and return, through their national interfaces or another form of access provided in the Union legal acts establishing such databases, as applicable. The host Member State may also authorise members of the teams to consult its national databases where necessary for the same purpose. Member States shall ensure that they provide such database access in an efficient and effective manner. Members of the teams shall consult only those data which are strictly necessary for performing their tasks and exercising their powers. The host Member State shall, in advance of the deployment of the members of the teams, inform the Agency of the national and Union databases which may be consulted. The Agency shall make this information available to all Member States participating in the deployment’.

Following Europol, the EBCG Agency is the Union body with the greatest access rights to large-scale IT systems and interoperability components. The ETIAS Central Unit has been granted access to the six large-scale IT systems⁷³⁴ to carry out the ETIAS automated checks and for carrying out the multiple-identity detection procedure during the MID transitional period⁷³⁵. The EBCG Agency is granted access to the SIS, the VIS⁷³⁶, the EES⁷³⁷, and the ETIAS⁷³⁸ to create statistics while the staff in charge of return-related tasks and the migration management support teams are also granted access to the SIS for return purposes⁷³⁹. Forced-return specialists are required for the ‘identification of particular groups of third-country nationals, the acquisition of travel documents from third countries and facilitation of consular cooperation’⁷⁴⁰. According to Article 27(1)(c) of the 2019 EBCG Agency Regulation, the agency must ‘coordinate the use of relevant IT systems and provide support to the Member States on consular cooperation for the identification of third-country nationals and the acquisition of travel documents, without disclosing information relating to the fact that an application for international protection has been made’. However, the SIS Regulations (EU) 2018/1861 and 2018/1862 prohibit the interconnection of the SIS ‘[...] to any system for data collection and processing operated by the teams referred to in paragraph 1 or by the European

⁷³³ Risk analyses are thought to give information on the whole aspects covered by the integrated border management concepts, including according to recital (18), Articles 9 and 10 of the 2016 EBCG Agency Regulation. As far as risk analysis is concerned, Article 11(3) specifies that these may flow into a pre-warning mechanism.

⁷³⁴ Articles 10(1)(f) and 67 of the 2019 EBCG Agency Regulation establish the ETIAS Central Unit within the own agency.

⁷³⁵ See Chapter V.

⁷³⁶ Articles 45a, 45d and 45e of the revised VIS Regulation.

⁷³⁷ Article 63(1) in fine of the EES Regulation.

⁷³⁸ Article 17(3) of the Regulation (EU) 2018/1860, Article 38 of the Regulation (EU) 2018/1861, and Article 50 of Regulation 2018/1862.

⁷³⁹ Article 36 of the Regulation (EU) 2018/1861 and Article 50 of the Regulation (EU) 2018/1862.

⁷⁴⁰ Article 31(1) of the EBCG Agency Regulation.

Border and Coast Guard Agency, nor shall the data in SIS to which those teams have access be transferred to such a system. No part of SIS shall be downloaded or copied [...]’⁷⁴¹.

The EBCG Agency can deploy information systems based on eu-LISA’s standards⁷⁴² and use existing communication networks with the purpose of exchanging classified and sensitive non-classified information, as well as personal data⁷⁴³. For example, the agency has implemented a reference model⁷⁴⁴ and a common platform⁷⁴⁵ in order to coordinate Member States’ Return CMSs. In addition, EUROSUR⁷⁴⁶ has been ‘upgraded’ from a technical information system to a governance framework for information exchange and cooperation. Therefore, not only has EUROSUR been converted into a communication network to improve information assurance between the Member States and with the agency⁷⁴⁷, but it also can be used for border checks and border surveillance, for legal and illegal migration, as well as to fight crime and mount rescue operations⁷⁴⁸. As for the former purpose, Member States are required to implement a national coordination centre that is responsible for coordinating the exchange of information: ‘The Agency should provide the necessary assistance for the development and operation of EUROSUR, including the interoperability of systems, in particular by establishing, maintaining and coordinating EUROSUR’⁷⁴⁹. The latter purpose, instead, allows EUROSUR to disclose pictures to the European Commission, the national coordination centres, and through the EUROSUR Fusion Services that include the monitoring of external borders and pre-frontier areas in order to: detect departures or transit involving illegal immigration or cross-border crimes; monitor migratory flows; undertake ‘media monitoring, open source intelligence and analysis of internet activities’ for the purpose of preventing illegal immigration or cross-border crime’, and analyse information derived from

⁷⁴¹ Article 36(7) of the Regulation 2018/1861 and Article 50(7) of the Regulation 2018/1862.

⁷⁴² Recital (19) and Articles 16 and 17 of the 2019 EBCG Agency Regulation. Also, see the EDPS Decision concerning *the investigation into Frontex’s move to the Cloud*, Brussels, 1.04.2022, assessing that the agency failed to conduct a timely and exhaustive assessment on the risks deriving from the movement of all its IT services to the Cloud.

⁷⁴³ Article 15 of the 2019 EBCG Agency Regulation.

⁷⁴⁴ Council of the EU, *Frontex Annual Activity Report 2017*, 10525/18, Brussels, 27 June 2018, p. 22.

⁷⁴⁵ Recital (83) of the 2019 EBCG Agency Regulation, and the Regulation (EU) 2020/493.

⁷⁴⁶ Article 18 ff. of the amended EBCG Agency Regulation.

⁷⁴⁷ Recital (28) and Article 22(2) of the 2019 EBCG Agency Regulation.

⁷⁴⁸ Article 19 of the amended EBCG Agency Regulation. Article 89 specifies the regime applicable to the personal data processing activities, namely the GDPR and the LED for the Member States and the LED for the EBCG Agency.

⁷⁴⁹ Recital 33 of the 2019 EBCG Agency Regulation.

large-scale information systems for the purpose of detecting changing routes and methods used for illegal immigration and cross-border crime⁷⁵⁰.

The regime on the protection of personal data foreseen under the 2019 EBCG Agency Regulation⁷⁵¹ pays special attention to people with special need or in vulnerable situations. It has established a fundamental rights officer responsible for handling complaints made against the agency and has confirmed the adoption of a code of conduct and undertakes specific trainings⁷⁵². Nevertheless, the legal framework on personal data applicable to the EBCG Agency remains highly complicated because of the ‘hybrid’ mandate of the agency. The regime established for the processing of personal data takes as a point of reference the EUDPR⁷⁵³ as far as the agency’s staff is concerned, while Member States’ authorities are subjected to the GDPR and the LED⁷⁵⁴. Significant exceptions are made *a priori* on Articles 14 to 22, 35 and 36⁷⁵⁵ of the EUDPR⁷⁵⁶, arguably in order to facilitate the return of third country nationals. However, Article 86(2), second paragraph, of the EUDPR specifies that any restriction should respect the essence of the fundamental rights and freedoms, shall be necessary and proportionate to the objectives pursued, and be set forth by law according to the provisions on restriction of the data subject’s rights by virtue of Article 25(2) EUDPR.

The EBCG Agency mandate sets forth the purposes for which personal data can be processed, in strict respect of the principle of proportionality, which essentially summarises the operational tasks assigned to the agency⁷⁵⁷, namely: organising and coordinating joint operations, pilot projects, rapid border interventions and the migration management support teams; supporting Member States and third countries in pre-return and return activities, operating return management systems, as well as coordinating or organising return operations and providing technical and operational assistance to Member States and third countries;

⁷⁵⁰ Article 28(2) of the 2019 EBCG Agency Regulation.

⁷⁵¹ Recital (49) of the 2019 EBCG Agency Regulation.

⁷⁵² Articles 35 and 26 of the 2019 EBCG Agency Regulation.

⁷⁵³ Recital (98) of the 2019 EBCG Agency Regulation.

⁷⁵⁴ Recital (98) of the 2019 EBCG Agency Regulation.

⁷⁵⁵ Transparent information, communication and modalities for the exercise of the rights of the data subject; information to be provided where personal data are collected from the data subject; information to be provided where personal data have not been obtained from the data subject; right of access by the data subject; right to rectification; right to erasure (‘right to be forgotten’); right to restriction of processing; notification obligation regarding rectification or erasure of personal data or restriction of processing; right to data portability communication of a personal data breach to the data subject, and confidentiality of electronic communications.

⁷⁵⁶ Article 86(2), second paragraph, of the 2019 EBCG Agency Regulation: ‘[...] the Agency may, for the performance of its tasks in the area of return, provide for internal rules restricting the application of those provisions on a case-by-case basis as long as the application of those provisions would risk jeopardising return procedures’.

⁷⁵⁷ Article 87 of the EBCG Agency Regulation.

facilitating the exchange of information with Member States, the European Commission, the European External Action Service and Union bodies, offices and agencies and international organisations with which it cooperates⁷⁵⁸; facilitating the exchange of information with the law enforcement authorities of the Member States, Europol or Eurojust; risk analysis; performing its tasks in relation to EUROSUR; operating the FADO system and, finally, administrative tasks. In the case of the EBCG Agency's joint operations, return operations, return interventions, pilot projects, rapid border interventions, and migration management support team deployments, the Regulation establishes that Member States' authorities and the agency staff must be considered as joint controllers '[w]hen the purpose and the means of processing are jointly determined by the Agency and the host Member State [...]'⁷⁵⁹. Specifically, Article 88(2) of the 2019 EBCG Agency Regulation addresses the following cases:

- personal data of individuals who cross the external borders without authorisation;
- personal data that is necessary to confirm the identity and nationality of third-country nationals in relation to return activities, including passenger lists, and
- licence plate numbers, vehicle identification numbers, telephone numbers or ship and aircraft identification numbers which are linked to individuals that cross the external borders without authorisation, and which are necessary for analysing the routes and methods used for illegal immigration.

This data can be used to support the EUAA, Europol, and Eurojust's activities and, in accordance with EU and national law, can be transmitted to the authorities competent for border control, migration, asylum or law enforcement⁷⁶⁰. It is worth noting that when the EBCG Agency processes personal data relating to its operations to identify cross-border crime suspects, it is not subject to the general provisions of the EUDPR, but rather to the specific provisions of Chapter IX of the EUDPR⁷⁶¹. According to Quintel:

'As quasi EU LEA, the EBCGA will play a decisive role as to the practical application of Regulation (EU)2018/1725 in terms of the delineation between the general rules (i.e. processing for migration management) and the provisions on operational data (i.e. certain situations when cooperation with Europol takes place). [...] Thereby, the EBCGA will set standards for the delineation between the rules applicable to LE- and non-LE processing under Regulation (EU)2018/1725 and could serve as model for processing by national LEAs (i.e. the delineation between the GDPR and the LED), as the rules on EU and national level are now aligned'⁷⁶².

⁷⁵⁸ See *infra*.

⁷⁵⁹ Article 88 of the 2019 EBCG Agency Regulation.

⁷⁶⁰ Article 88(2) of the 2019 EBCG Agency Regulation.

⁷⁶¹ Article 90 of the 2019 EBCG Agency Regulation.

⁷⁶² Teresa Quintel, 2020, *op. cit.*, p. 217.

Among the latter group, the data of suspects and victims or witnesses requires special care and can only be exchanged with Eurojust, Europol, and domestic competent authorities of law enforcement. This data ‘shall be deleted as soon as the purpose for which they have been collected has been achieved by the Agency’ or at least six months after the date of the initial processing⁷⁶³, which is the longest time limit for the storage period, recalling that in case of transmission of personal data – both in intra and extra institutional environments – the deadline is ninety days, or thirty days are allowed when performing return-related tasks. We agree with the author when she maintains that the simultaneous application of various provisions having different impacts on the individuals’ rights to the protection of personal data may be controversial as there is not a clear delineation between the GDPR, the LED, and the corresponding provisions of the EUDPR⁷⁶⁴. This may lead to abuses by the agency as guarantees are less stringent in the case of PJCCM activities.

2.3.2. The conclusion of arrangements and agreements under the EBCG Agency Regulation

The EBCG Agency is one of the AFSJ agencies that has contributed the most to experiments regarding the exercise of external operational competences⁷⁶⁵. Since 2008, the EBCG Agency has adopted a ‘network’ strategy, where it looks for strategic partners in various fields involved in border management activities and which can contribute to improving the management of the external borders of the EU⁷⁶⁶. Thus, its partners are active in fields such as security, immigration

⁷⁶³ Article 91(3) of the 2019 EBCG Agency Regulation.

⁷⁶⁴ See Chapter I.

⁷⁶⁵ Juan Santos Vara, 2014, “Análisis del marco jurídico-político de la dimensión exterior de las agencias del espacio de libertad, seguridad, y justicia”, *op. cit.*, p. 22 ff.

⁷⁶⁶ Although we are not here analysing the agency’s intra-institutional relations, we should recall that these are regulated under Article 68 of the 2019 EBCG Agency Regulation that refer to: the European Commission and the European External Action Service; Europol; the EUAA; the FRA; Eurojust; the European Union Satellite Centre; European Fisheries Control Agency and European Maritime Safety Agency; eu-LISA; the European Union Aviation Safety Agency and the Network Manager of the European Air Traffic Management Network, and Common Security and Defence Policy missions and operations, in accordance with their mandates, with a view to ensuring the following: (i) the promotion of European integrated border management standards; and (ii) situational awareness and risk analysis. Historically, the EBCG Agency has collaborated with Europol, European anti-fraud office, the Police Chiefs’ Task Force and other ‘actors at Community level responsible for customs, veterinary and other controls at the external border’. The EBCG Agency has concluded nine working arrangements with EU agencies and bodies, that is with: CEPOL; EUAA; European External Action Service; European Maritime Safety Agency and European Fisheries Control Agency; eu-LISA; Eurojust; Europol; FRA, and European Union Military Operation in the Mediterranean IRINI. These working arrangements are subject to the European Commission’s prior approval, plus the information to the European Parliament and the Council of the EU and, importantly, they may regulate for the transfer of personal data. With Europol, specifically, the EBCG Agency has undertaken a project on the fight against document frauds – see the Council of the EU, 10910/17, Brussels, 7 July 2017, p. 4 – and has signed a binding operational agreement – see the EBCG Agency-Europol Agreement, 4 December 2015, available at www.frontex.europa.eu. Also, Europol, the EUAA, the European Maritime Safety Agency, the European Union Satellite Centre, the European Authority for aviation safety, and the Network Manager of the European air traffic management network are important partners in this frame as they are supposed ‘to make the

and asylum, customs, maritime affairs, transport, technology, and crisis management⁷⁶⁷. The agency's operational activity must be consistent with other relevant EU policies and it is supposed to cover both a horizontal and a vertical dimension: the former is directed at controlling borders and, originating in the Member States it passes through neighbouring countries until reaching the origin and transit states⁷⁶⁸; the latter aims at enhancing inter-agency cooperation and comprehensive action in related fields such as crime prevention⁷⁶⁹. As the Regulation clearly expresses:

‘The establishment of cooperation with third countries shall serve to promote European integrated border management standards’⁷⁷⁰.

As a result, the EBCG Agency dedicates special attention to neighbouring countries that include future EU Member States – as has previously happened with Bulgaria and Romania –, candidate States – as with Croatia and Turkey⁷⁷¹ and now Albania –, Western Balkan countries⁷⁷², and Eastern Partners – e.g., Ukraine and Georgia – where the agency has been promoting the EU integrated border management model. Conversely, with countries of origin and transit⁷⁷³ the EBCG Agency follows the political dialogue underpinned by the EU with key African countries including: Cape Verde; Ghana; Mauritania, and Senegal as well as with the ECOWAS⁷⁷⁴. The dialogue with Southern Neighbourhood and West Africa partners was enhanced in 2019 with the Frontex-Morocco *Comité Mixte*⁷⁷⁵ while the cooperation with

best use of information, capabilities and systems which are already available at European level, such as Copernicus, the Union Earth observation and monitoring programme’ – recital (86) of the 2019 EBCG Agency Regulation.

⁷⁶⁷ Council of the EU, *FRONTEx Annual Report*, 12305/09, Brussels, 24 July 2009, p. 17.

⁷⁶⁸ The EBCG Agency has progressively absorbed the activity deployed by three EU networks financed by Asylum, Migration and Integration Fund for the development of an “Integrated Return Management System”. These networks are: the European Integrated Return Management Initiative network; the European Return Liaison Officers’ network, and the European Reintegration Network, which became the European Return and Reintegration Network with expanded scope in 2018 – confront the Court of Auditors, *EU readmission cooperation with third countries: relevant actions yielded limited results*, Luxembourg, 2021, p. 41.

⁷⁶⁹ Council of the EU, *Frontex Programme of Work 2010*, 6674/10, Brussels, 23 February 2010, p. 32.

⁷⁷⁰ Article 71(4) of the 2019 EBCG Agency Regulation.

⁷⁷¹ Council of the EU, *FRONTEx Annual Report 2006*, 11691/07, Brussels, 12 July 2007, p. 19.

⁷⁷² Council of the EU, 5685/08, Brussels, 15 February 2008. Notably, in the Western Balkan the agency is carrying out a project “Regional support to protection sensitive migration management in the Western Balkans and Turkey” together with the EUAA, the IOM, and the UNHCR whose second phase is directed at reinforcing migration management capacities for identification, registration, referral, asylum, and return. National coordination centers apart, the EBCG Agency is developing ‘national registration systems with the view to facilitate in the future their eventual interoperability with EURODAC in the context of the EU accession’. Also, the EBCG Agency hosted Western Balkan’s experts in 2019 to ‘get hands-on experience on advance passenger information systems in the EU with a view to support the implementation of Advance Information systems at national level’ – see the Council of the EU, *Frontex Annual Risk Analysis 2021: The Cross-Border Crime dimension with the angle of the external borders*, 7233/21, Brussels, 25 March 2021, pp. 18 and 19.

⁷⁷³ See the Council of the EU, 12049/06, Brussels, 20 November 2006, p. 10.

⁷⁷⁴ Council of the EU, 11691/07, Brussels, 12 July 2007, p. 18.

⁷⁷⁵ Council of the EU, *Report on cooperation between Frontex, the European Border and Coast Guard Agency and third countries in 2019*, 8896/20, Brussels, 17 June 2020.

Turkey is still a “work in progress” between the EBCG Agency’s liaison officers deployed in Ankara and the Turkish representatives participating in the agency’s events and activities. The agency’s external strategy was split in order to cover the Mediterranean area, West Africa, Central Asia, and the Far East, but it has progressively expanded overseas to the US, Canada⁷⁷⁶, Australia, New Zealand, and China in the light of the ETIAS⁷⁷⁷ from which it receives “familiarisation visits”.

a) The EBCG Agency’s working arrangements

The agency’s cooperation with third countries is mainly channelled⁷⁷⁸ through working arrangements⁷⁷⁹ that include the commitment to:

- exchange information, including personal data;
- elaborate and coordinate joint operations and pilot projects, as well as to
- cooperate for risk analysis, technical development in border controls and the execution of those controls.

We support the idea that these arrangements are the agency’s own arrangements⁷⁸⁰ with a soft law character, as it is affirmed in the clause establishing that they are not intended to produce juridical effects on third parties which implies, among others, that they cannot be

⁷⁷⁶ Council of the EU, *FRONTEx work programme 2007*, 6642/07, Brussels, 22 February 2007, p. 14 ff. See also the European Court of Auditors, *EU readmission cooperation with third countries: relevant actions yielded limited results*, Luxembourg, 2021, that show how the negotiation by the European Commission with third countries of origin and transit of soft arrangements is more effective than the one of binding readmission agreements because of their flexibility that meets foreign partners’ political will. These arrangements are negotiated by the Commission authorised by the Council that has also to confirm the outcome. However, and differently from the procedure required for the conclusion of an EU readmission agreement, the consent of the European Parliament is not required. The arrangements are monitored by Joint Working Groups but are not published except the one with Afghanistan available at www.eeas.europa.eu.

⁷⁷⁷ Council of the EU, 8896/20, Brussels, 17 June 2020, p. 7.

⁷⁷⁸ The agency collaborates with other networks like the International Border Police Conference, and the EU Situation Centre, and the Baltic Sea Region Border Control Cooperation. Confront the Council of the EU, *Frontex Work Programmes 2005 and 2006*, 6941/06, Brussels, 11 July 2006, p. 9.

⁷⁷⁹ To be noted that the 2011 Regulation clarified that with the conclusion of working arrangements, Frontex could have transmitted or communicated personal data to other EU agencies – such as Europol, EASO and FRA – and international organisations ‘within the framework of working arrangements concluded with those bodies, in accordance with the relevant provisions of the TFEU and the provisions on the competence of those bodies’, although the founding Treaties did not foresee any disposition on the conclusion of soft-law instrument. See the EDPS disappointment because of the lack of reference to personal data in the exchange of information – specifically, through the working arrangements – with third parties in the European Commission in Council of the EU, 10127/10, Brussels, 25 May 2010, p. 10.

⁷⁸⁰ Working arrangements specify that they have no binding nature, and they are not treaty under international law, which excludes the possibility to bind the EU as well as to recognise the EBCG Agency international legal personality. Notably, they also state that they do not constitute an implementation of EU international obligations with the exception of the EBCG Agency-MARRI Regional Centre in the Western Balkans working arrangement that are silent on this point.

subjected to the CJEU's control⁷⁸¹. Indeed, the EBCG Agency's working arrangements are adopted by the Management Board by absolute majority, after the European Commission's prior approval and after having informed the European Parliament and the Council⁷⁸². They are finally signed by the Executive Director⁷⁸³ who re-consults the European Commission together with the Member States and submits the draft mandate to the Management Board.

The EBCG Agency counts on twenty – published⁷⁸⁴ – working arrangements⁷⁸⁵ concluded with third countries, the Commonwealth of independent states, and the Migration, Asylum, Refugees Regional Centre in the Western Balkans⁷⁸⁶. The third countries and organisations in question are: Albania⁷⁸⁷, Armenia⁷⁸⁸, Azerbaijan⁷⁸⁹, Belarus⁷⁹⁰, Bosnia and Herzegovina⁷⁹¹, Canada⁷⁹², Cape Verde⁷⁹³, the Coordination Service of the Commonwealth of Independent States Border Commandants' Council⁷⁹⁴, Georgia⁷⁹⁵, Kosovo⁷⁹⁶, Moldova⁷⁹⁷, Montenegro⁷⁹⁸,

⁷⁸¹ T-411/06, *Sogelma – Società generale lavori manutenzione appalti Srl v European Agency for Reconstruction (EAR)*, 8 October 2008, EU:T:2008:419. In this sense see Jorrit J. Rijpma, *Building Borders: The Regulatory Framework for the Management of the External Borders of the European Union*, Ph. D. dissertation, EUI (Fiesole), 2009, p. 333, and Melanie Fink, "Frontex Working Arrangements: Legitimacy and Human Rights Concerns Regarding 'Technical Relationship'", *Utrecht Journal of International and European Law*, Vol. 28, No. 75, 2012, pp. 20-35.

⁷⁸² According to Juan Santos Vara, "External Activities of AFSJ Agencies: The Weakness of Democratic and Judicial Controls", *European Foreign Affairs Review*, No. 1, Vol. 20, 2015, pp. 115-136, p. 125: 'Given the implications that Frontex's working arrangements may have for human rights, they should be subject to the prior approval of Parliament'.

⁷⁸³ See the Management Board Decision No. 11 of 30 March 2017 adopting the Rules of Procedures of the Management Board, Reg. No. 5792, available at www.frontex.europa.eu.

⁷⁸⁴ According to Luisa Marin, "The Cooperation Between Frontex and Third Countries in Information Sharing: Practices, Law and Challenges in Externalizing Border Control Functions", *European Public Law*, Vol. 26, No. 1, 2020, pp. 157-180, other arrangements and other forms of cooperation have been established by the agency but they are not all published. For example, the author points out that the Africa-Frontex Intelligence Community was set up in 2010 to provide the regular knowledge and intelligent sharing with key African countries which was formalised only subsequently, under Article 54(9) of the 2016 EBCG Agency Regulation.

⁷⁸⁵ All the working arrangements are available at www.frontex.europa.eu.

⁷⁸⁶ EBCG Agency-Migration, Asylum, Refugees, Regional Initiative Regional Centre in the Western Balkans working arrangement (the date is not specified).

⁷⁸⁷ EBCG Agency-Republic Albania working arrangement of 17 March 2021.

⁷⁸⁸ EBCG Agency-Republic of Armenia working arrangement of 22 February 2012.

⁷⁸⁹ EBCG Agency- Azerbaijan working arrangement of 16 April 2013.

⁷⁹⁰ EBCG Agency-Republic of Belarus working arrangement of 21 October 2009.

⁷⁹¹ EBCG Agency-Bosnia and Herzegovina working arrangement of 3 April 2009.

⁷⁹² EBCG Agency-Canada working arrangement of 21 October 2010.

⁷⁹³ EBCG Agency-Cape Verde working arrangement of 14 January 2011.

⁷⁹⁴ EBCG Agency-Coordination Service of the Commonwealth of Independent States Border Commandants' Council working arrangement of 16 December 2010.

⁷⁹⁵ EBCG Agency-Georgia working arrangement of 11 February 2021.

⁷⁹⁶ EBCG Agency-Kosovo working arrangement of 25 May 2016.

⁷⁹⁷ EBCG Agency-Moldova working arrangement of 12 August 2008.

⁷⁹⁸ EBCG Agency-Montenegro working arrangement of 12 June 2009.

Nigeria⁷⁹⁹, Serbia⁸⁰⁰, the former Yugoslav Republic of Macedonia⁸⁰¹, the Russian Federation⁸⁰², the United States⁸⁰³, Turkey⁸⁰⁴, and Ukraine⁸⁰⁵. These working arrangements do not share the same structure, but some common points may be highlighted.

Two main fields of cooperation are agreed under working arrangements for which purpose the EU may provide financial support to the other side. These fields are: integrated border management – including the fight against cross-border crimes –, and the countering and returning of irregular migrants. In some working arrangements⁸⁰⁶, the sides promote ‘the improvement of the operational interoperability between the competent authorities involved in border management activities and commit to respect international human rights by paying attention to specific groups of people like international protection seekers, unaccompanied minors, and other vulnerable persons’. The exchange of information constitutes one of the main modalities of cooperation undertake to expand situational awareness and joint risk analysis and partners include the Western Balkans Risk Analysis Network, the Eastern Partnership Risk Analysis Network, the Turkey-Frontex Risk Analysis Network, and the Africa-Frontex Intelligence Community⁸⁰⁷, who may exchange information in order to:

- improve border management and the return system;
- create periodical statistics and other situational awareness products as well as situation monitoring and operational media monitoring products and services, all of them related to border management, irregular migration and cross-border crime;
- address new challenges in the area of border security, fighting against irregular migration, cross border crime and terrorism as well as related *modi operandi*;
- evaluate the migratory routes and other relevant information related to the fight against cross-border criminality and the return of illegally staying third country nationals;
- prevent strategies and management methods to define border security priorities, and
- improve inter-service coordination, as well as threat assessments, risk analyses and situation reports.

⁷⁹⁹ EBCG Agency-Nigeria working arrangement of 19 January 2012.

⁸⁰⁰ EBCG Agency-Serbia working arrangement of 17 February 2009.

⁸⁰¹ EBCG Agency-former Yugoslav Republic of Macedonia (the date is not specified).

⁸⁰² EBCG Agency-Russian Federation of 14 September 2006.

⁸⁰³ EBCG Agency-USA of 28 April 2009.

⁸⁰⁴ EBCG Agency-Turkey of 28 May 2012.

⁸⁰⁵ EBCG Agency-Ukraine of 11 June 2007.

⁸⁰⁶ That are the EBCG Agency-Republic Albania, -Georgia, -Kosovo, and -Nigeria working arrangements.

⁸⁰⁷ Council of the EU, 8896/20, Brussels, 17 June 2020, p. 10.

The majority of the working arrangements do not specify whether ‘operational personal data’ can be exchanged under the aegis of such a soft arrangement: the possibility of such must be interpreted by the wording used therein. An exception is made for the working arrangements concluded with Canada⁸⁰⁸, the US, and the Migration, Asylum, Refugees Regional Initiative Regional Centre in the Western Balkans. Those involving Canada and US are interesting regarding other fields of cooperation such as technologies and research including mobile biometric data collection, and capacity building in third countries⁸⁰⁹. Prof. Marin highlights⁸¹⁰ that with some countries – namely Albania, Bosnia, Cape Verde, Macedonia, Montenegro, Nigeria, Serbia – the flow of information can be described as one-way road, that is, it is directed at providing the EBCG Agency with analytical data in exchange for technical assistance and funding⁸¹¹. In addition, working arrangements do anticipate the possibility to exchange ‘administrative data’ and impose the duty to respect the respective legal frameworks on data protection while limiting the usage of data to the purposes outlined by each arrangement. Further agreements, such as those on cross-border criminality, classified information⁸¹², or capacity building activities are agreed separately.

The EBCG Agency’s working arrangements enable third country authorities to take part in the EBCG Agency’s meetings and activities as observers, while the EBCG Agency is allowed to deploy its teams with non-executive powers in the Joint Coordination Points temporally activated in third countries’ territories according to a specific operational plan. In addition, recent working arrangements foresee the possibility of the EBCG Agency deploying liaison officers without executive powers so as to provide technical and operational assistance, while the other side can second observers to the agency’s headquarters and participate in expert activities⁸¹³. The EBCG Agency may be granted the use of the other side’s seaports and airports to, for example, support border surveillance as well as conduct search and rescue operations, with naval and aerial assets, including the deployment of maintenance staff. The

⁸⁰⁸ Article 4(ii) of the EBCG Agency-Canada working arrangement, according to which: ‘[...] This Working Arrangement does not authorise nor require the transmission of personal information or data, as defined under the relevant legal framework applicable to each Participant, related to an identified individual or identifiable individuals’.

⁸⁰⁹ Article 4(vii) of the EBCG Agency-Canada working arrangement, and 4(G) and (H) of the EBCG Agency-US working arrangement.

⁸¹⁰ Luisa Marin, *op. cit.* p. 166 ff.

⁸¹¹ *Ibid.*, p. 167: ‘Overall, the process seems to be one of construction of a buffer zone of countries that work according to the EU’s needs in order to cooperate with EU countries in the management of the external borders’.

⁸¹² Article 74(3), third paragraph, specifies that the exchange of classified information is regulated by Article 76(4) of the 2019 EBCG Agency Regulation and that the EDPS must be consulted in case these working arrangements provide for the transfer of personal data.

⁸¹³ Article 74 of the 2019 EBCG Agency Regulation.

implementation of the working arrangement may be subjected to a ‘dialogue’ established among the two sides and, specifically, among their designated specific contact points. Eventually, expert working groups can be established to address specific issues and to craft recommendations. In addition, the agency is allowed to: send return specialists, share best practices, hold workshops for the consular offices, and deploy pilot projects in the so-called pre-return phase. For example, a pilot project was developed concerning the implementation of a system identifying migrants in cooperation with European Return Liaison Officers Network and IOM, though three quarters of those identified applied for international protection and were not returned. Cooperation activities with third countries include coordination and financing of visits by third-country officials – “identification missions” – for identification purposes and to facilitate the issuance of travel documents as well as various meetings with third-country authorities – e.g., sensitisation missions⁸¹⁴ –:

‘Member States developed the concept of identification missions to address issues with consular cooperation with third countries (e.g. when a consulate does not want to cooperate on identification, does not have the mandate to do so, or is not physically present in a Member State). Frontex has been supporting Member States with identification missions since the end of 2016, when it took this activity over from Eurint. The Frontex support is driven by requests from Member States, and its exact form is defined on a case-by-case basis’⁸¹⁵.

The 2019 EBCG Agency Regulation⁸¹⁶ clarifies that Member States are free to conclude bilateral or multilateral agreements, other forms of arrangements, or operate through regional networks established on the basis of those agreements that include the exchange of information with third parties⁸¹⁷. However, they are required to respect Union and international law on fundamental rights and on international protection, including the CFREU, the ECHR and the 1951 Geneva Convention, its 1967 Protocol, and in particular the principle of *non-refoulement*. They are also called to sincerely cooperate with the agency and to ‘[...] refrain from any activity

⁸¹⁴ Council of the EU, 5247/18, Brussels, 30 January 2018, p. 78.

⁸¹⁵ European Court of Auditors, *EU readmission cooperation with third countries: relevant actions yielded limited results*, Luxembourg, 2021, p. 44.

⁸¹⁶ Article 8(2) of the 2016 EBCG Agency Regulation was stricter as it sounds now:

‘Member States shall refrain from any activity which could jeopardise the functioning of the Agency or the attainment of its objectives. Member States shall report to the Agency on that operational cooperation with other Member States and/or third countries at the external borders and in the field of return. The executive director shall inform the management board on those matters on a regular basis and at least once a year’.

Also, it stated that when concluding bilateral agreements with third countries, Member States might include provisions concerning the role and competence of the agency in accordance with its mandate, in particular regarding the exercise of executive powers by members of the EBCG teams deployed by the agency during the joint operations, pilot projects, rapid border interventions, return operations, or return interventions. The Member States should have notified the European Commission of any such provisions – see Article 54(8) and (10) of the 2019 EBCG Agency Regulation.

⁸¹⁷ Article 72 of the 2019 EBCG Agency Regulation.

which could jeopardise the functioning of the Agency or the attainment of its objectives'⁸¹⁸. Notably, the EU legislator invited the Member States to insert provisions regarding the EUROSUR in their bilateral and multilateral agreements to facilitate the gathering of updated information on third countries⁸¹⁹.

The transfer of personal data by the agency to international organisations is regulated by Article 87(1)(c) of the 2019 EBCG Agency Regulation to which data protection provisions laid down in Section 2 of Chapter IV apply. In particular, the agency shall ensure that any working arrangement concluded with international organisations regarding the exchange of personal data under point (c) of Article 87(1) complies with Chapter V EUDPR and is subject to the authorisation of the EDPS, where provided for by that Regulation. The agency should ensure that personal data transferred to international organisations is only processed for the purposes for which it was transferred. The international organisations, for their part, must use the information received within the limits of their competence and in respect of fundamental rights, including the protection of personal data. Such an exchange is realised through the agency's own communication network⁸²⁰.

Article 68(1), second paragraph, foresees that the EBCG Agency can conclude working arrangements with:

- the United Nations through its relevant offices, agencies, organisations, and other entities, in particular the Office of the UNHCR, the Office of the High Commissioner for Human Rights, the IOM, the United Nations Office on Drugs and Crime, and the International Civil Aviation Organisation;
- Interpol;
- the Organisation for Security and Cooperation in Europe;
- the Council of Europe and the Commissioner for Human Rights of the Council of Europe, and
- the Maritime Analysis and Operations Centre — Narcotics.

The conclusion of working arrangements is subject to the European Commission's prior approval and the notification to the European Parliament and the Council of the EU. As of

⁸¹⁸ Article 7(5) of the 2019 EBCG Agency Regulation.

⁸¹⁹ Recital (90) of the 2019 EBCG Agency Regulation:

'[...] the Agency should cooperate with the authorities of third countries either in the framework of bilateral and multilateral agreements between the Member States and third countries, including regional networks, or through working arrangements concluded between the Agency and the relevant authorities of third countries. For those purposes, the European External Action Service and Union delegations and offices should provide all information that could be relevant for EUROSUR'.

⁸²⁰ Article 14 of the 2019 EBCG Agency Regulation.

today, eight working arrangements are in force with the following international organisations and bodies: the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation⁸²¹; the Centre for Security Development and the Rule of Law⁸²²; the International Centre for Migration⁸²³; Interpol⁸²⁴; IOM⁸²⁵; the Organisation for Security and Co-operation in Europe⁸²⁶; UNHCR⁸²⁷, and United Nations Office on Drugs and Crime⁸²⁸. Each agreement reflects the specific interests the EBCG Agency has with regard to the fields of competences covered by the international organisation it is dealing with; yet, unlike the working arrangements concluded with third countries, they do not explain whether the agreements have a soft or hard nature.

The EBCG Agency-European Committee for Standardisation and EBCG Agency-Committee for Electrotechnical Standardisation working arrangements foresees the possibility for the EBCG Agency to attend the meetings of the other side and imposes on the EBCG Agency a duty to respect the norms on intellectual property rights held by the European Committee for Standardisation and European Committee for Electrotechnical Standardisation. The EBCG Agency-Geneva Centre for Security Sector Governance working arrangement provides for ‘effective cooperation and liaisons’ between the two sides in the border management field through the exchange of information and joint training activities. The EBCG Agency-Centre for Security Development and the Rule of Law working arrangement aims at fostering cooperation in the promotion, development, and implementation of integrated border management projects, which includes the exchange of information and, in exceptional cases, of personal ‘sensitive data’ relating to specific projects.

Since 2016, the EBCG Agency and Interpol have been collaborating in the Frontex-Interpol Electronic Library Document System project, a police communication network that facilitates front-line law enforcement officers in travel and ID document checks⁸²⁹. Notably, the EBCG-Interpol working arrangement does not mention whether it has soft nature or not⁸³⁰. It is

⁸²¹ EBCG Agency-European Committee for Standardization and European Committee for Electrotechnical Standardisation working arrangement (the date is not specified).

⁸²² EBCG Agency-Geneva Centre for Security Sector Governance working arrangement (the date is not specified).

⁸²³ EBCG Agency-International Centre for Migration Policy Development of 4 June 2009.

⁸²⁴ EBCG Agency-Interpol working arrangement of 27 May 2009.

⁸²⁵ EBCG Agency-IOM working arrangement of 1 July 2008.

⁸²⁶ EBCG Agency-Organization for Security and Co-operation in Europe working arrangement of 17 October 2019.

⁸²⁷ EBCG Agency-UNHCR working arrangement, 16 June 2008.

⁸²⁸ EBCG Agency-United Nations Office on Drugs and Crime working arrangement of 17 April 2012.

⁸²⁹ Council of the EU, 7233/21, Brussels, 25 March 2021, p. 14.

⁸³⁰ Andrea Ott, Ellen Vos, and Florin Coman-Kund, 2014, *op. cit.*, p. 34: ‘Hence, this seems to be a binding action that is breaching EU primary law (Articles 218 and 220 TFEU) and the *Meroni* doctrine, as contrary to the

specifically directed at combating cross-border crimes or specific target activities in the fields of illegal immigration, smuggling of people, and trafficking in human beings. The means of cooperation include the exchange of information, including personal data, and documents of common interest. The working arrangement distinguishes between ‘strategic information’ and ‘technical information’, but it does not specify whether this includes personal data and, if so, which types. The provision of information is regulated by each side’s legal framework, yet they must both forward reliable and up-to-date information while informing of possible modifications or the deletion of data. In any case, the processing of information must stay within the scope of the agreed working arrangement and onward transfers must be authorised by the other side. It is up to each side to ensure that those in charge of the processing meet the requisites imposed by the correspondent legal framework.

The EBCG Agency-IOM working arrangement is focused on migration and border management and includes the exchange of relevant information and documentation with the exception of personal data. In regard to specific projects or programs it may be possible, instead, to exchange ‘operationally sensitive data’ under a reciprocal agreement on its necessity.

The EBCG Agency-Organisation for Security and Co-operation in Europe working arrangement aims at establishing cooperation among parties in the fields of integrated border management, specifically for the managing of migration and serious crimes. The working arrangement distinguishes it from the other working arrangements as it pays specific attention to gender equality in border security and management, and it provides the leadership of border security and management organisations with a platform for information exchange, cooperation, and coordination. The exchange of information includes the sharing of analytical products and of analysis and situational information. The exchange of personal data is prohibited except for ‘administrative purposes’ necessary for the implementation of the working arrangement. In addition, the exchange and transfer of ‘data and information’ is subjected to the respective legal frameworks, for which purpose they must abide by handling codes, including access restrictions, specific terms, and deletion or destruction periods. The exchange of data and information is conducted by the respective contact points, namely the Frontex Institutional Partnership Unit and Organisation for Security and Co-operation in Europe Transnational Threats Department.

European Commission’s role *vis-à-vis* European Authority for aviation safety’s actions, the role of the European Commission in these actions is not clarified’, which is probably due to the disputes surrounding Interpol’s international legal personality – see Henry G. Schermers and Niels M. Blokker, *International Institutional Law: Unity within Diversity*, Boston, Martinus Nijhoff Publishers, 2011, p. 40.

The EBCG Agency-UNHCR working arrangement is directed at respecting the principle of non-refoulement and international protection seekers in the management of external borders. For this purpose, the parties can exchange information, e.g., on migratory movements, as well as that gathered in respect of joint operations.

Finally, the EBCG Agency-United Nations Office on Drugs and Crime working arrangement is directed at establishing cooperation ‘focused but not limited to border management and related transnational organized crime as defined in the respective mandates of the Organisations’. Any exchange of information is subjected to the respective legal framework of the agency and the United Nations Office on Drugs and Crime and must fall within the scope of the working arrangement. Specifically, the arrangement is ‘without prejudice to the relevant provisions applicable to Frontex concerning classified information, protection of personal data and public access to documents of EU bodies’⁸³¹. As a result, the EBCG Agency may submit a notification of any communication of restricted data to the United Nations Office on Drugs and Crime contact point.

b) The conclusion of status agreements

If the EBCG Agency foresees the deployment of teams in third countries where they are authorised to exercise coercive powers, then, the EU must conclude a status agreement by virtue of Article 218 TFEU⁸³². Status agreements cover all relevant aspects necessary to achieve the project’s goals, which include the provisions on the exchange of information and the transfer of personal data the EDPS should be aware of. These agreements recall the communitarisation of Europol and Eurojust’s cooperation agreements provided that the agency⁸³³ has a ‘mixture of intergovernmental and supranational control’⁸³⁴ which turns it into a ‘dual identity’ agency⁸³⁵. However, it is important to note that the European Commission – and not the Council of the EU – plays a significant role in the creation of the corresponding draft model, as well as during the negotiations⁸³⁶, of these status agreements.

Most important are those countries that constitute a country of origin or transit regarding illegal immigration⁸³⁷ since the EBCG Agency’s liaison officers are supposed to prevent illegal

⁸³¹ Article 2(1) of the EBCG Agency-United Nations Office on Drugs and Crime working arrangement.

⁸³² Article 73(3) of the 2019 EBCG Agency Regulation.

⁸³³ Indeed, the EBCG Agency also cooperates in operational action within the European Multidisciplinary Platform Against Criminal Threats as stated in the Council of the EU, 7233/21, Brussels, 25 March 2021, p. 13.

⁸³⁴ Melanie Fink, *loc. cit.*

⁸³⁵ Jorrit J. Rijpma, *op. cit.*, p. 528.

⁸³⁶ Article 76 of the 2019 EBCG Agency Regulation.

⁸³⁷ Article 77(2) of the 2019 EBCG Agency Regulation.

immigration and facilitate the return of third country nationals illegally staying in the EU. Still in regard to the deployment of the EBCG Agency liaison officers in third countries, the parties shall agree an operational plan that may include provisions concerning the exchange of information and cooperation for the purpose of EUROSUR⁸³⁸. The EBCG Agency deploys liaison officers to provide technical and operational assistance while third countries – and international organisations – may second observers to the agency’s headquarters to participate in joint operations, pilot projects, risk analysis, and training⁸³⁹. The EBCG Agency’s Immigration liaison officers can be deployed in EU delegations to third countries under the condition that the foreign country complies with ‘minimum human rights standards’ and will closely coordinate their work with the European migration liaison officers, the immigration liaison officers of the EU Member States, and other actors⁸⁴⁰. The EBCG Agency’s diplomatic activity is subjected to EU norms and standards, including the respect of fundamental rights and human dignity, when it acts in third countries⁸⁴¹ where it is expected to promote EU fundamental rights, including personal data protection and the principle of non-refoulement, within their operational activity⁸⁴². When its agents are authorised to use coercive powers, then, status agreements are legally binding and enforceable instruments that shall include appropriate safeguards for individuals.

The European Commission was called on to draft a model of status agreement⁸⁴³ that would be subject to the EDPS’ approval⁸⁴⁴. The latter complained about various dispositions on the processing of personal data found in the different forms of collaboration – e.g., the invitation of foreign observers to expert activities, or cooperation in identifying third country nationals present in the territory of a Member State or an Associated Country for the purposes of return⁸⁴⁵. The EDPS affirmed that the model lacked “essential data protection safeguards” and should have been developed further in order to comply with EU law.

⁸³⁸ Articles 74(6) and 75 of the 2019 EBCG Agency Regulation.

⁸³⁹ Articles 74 and 87 of the 2019 EBCG Agency Regulation.

⁸⁴⁰ Frontex liaison officers were established by the Council Regulation (EC) 377/2004 of 19 February 2004 on the creation of an immigration liaison officers network, *OJ L* 64, 2.3.2004, pp. 1-4, and their regime was revisited with the Regulation (EU) 493/2011 of the European Parliament and of the Council of 5 April 2011 amending Council Regulation (EC) No 377/2004 on the creation of an immigration liaison officers network, *OJ L* 141, 27.5.2011, pp. 13-16. The first the EBCG Agency liaison officers was deployed in Ankara, Turkey, in 2016.

⁸⁴¹ Article 14 of the Frontex amended Regulation.

⁸⁴² Articles 71(2) and 73(3) of the 2019 EBCG Agency Regulation.

⁸⁴³ Article 76(1) of the 2019 EBCG Agency Regulation.

⁸⁴⁴ Article 76(2) of the 2019 EBCG Agency Regulation.

⁸⁴⁵ Comments of the EDPS on *the model for working arrangements to be concluded by the European Border and Coast Guard Agency with the authorities of third countries*, Brussels, 3.07.2020, in which it specified that the approval of the model would have not substituted the necessary approval EDPS shall issue on each proposed working agreement, p. 3.

If a status agreement exists, the EBCG Agency may further conclude a working arrangement that refers to it and, if necessary, provide for further details for the implementation of those safeguards. Yet, in the absence of a status agreement, or if the status agreement does not aim at regulating personal data processing, or if it does not contain comprehensive and sufficient data protection safeguards, a working arrangement *per se* is considered to be a valid legal basis for the transfer of personal data. In this regard, the EDPS expressly refers to Article 48(3) (b) EUDPR and Article 73(4) of the 2019 EBCG Agency Regulation: the latter authorises the agency to conclude working arrangements with third countries on the exchange of sensitive non-classified information, on EUROSUR, as well as on classified information⁸⁴⁶. These working arrangements must be communicated to the European Parliament with detailed information regarding the parties and the agreement's envisaged content⁸⁴⁷.

At present, the EU concluded status agreements with Albania in 2018, Montenegro and Serbia in 2019, as well as with Moldova in 2022 following the Russian invasion of Ukraine⁸⁴⁸. As part of the joint operation, the EBCG teams deployed in the third country's territories are able to consult national databases for the purpose of returning irregular migrants. As a result, status agreements provide for a clause on the protection of personal data specifying that while the third country is subject to its national law, the EBCG Agency's teams shall respond to the EUDPR provisions, and officials from Member States shall respond to the GDPR and the LED's provisions. These regimes are also valid in cases of a transfer of personal data to foreign competent authorities, for which purpose the deployed team may communicate the existence of restrictions in the processing of personal data. The provision concerning administrative personal data is vaguer, as it merely points out that they '[...] may be processed by the Agency, the participating Member States and the Republic of Albania in line with the applicable data protection law', which does not clarify which regime is actually applicable. These activities are

⁸⁴⁶ The latter is regulated by Article 76(4) for which the European Commission shall be notified to give its prior approval.

⁸⁴⁷ Article 74(3), instead, regulates the technical and operational assistance to third countries.

⁸⁴⁸ Council Decision (EU) 2019/267 of 12 February 2019 on the conclusion of the Status Agreement between the European Union and the Republic of Albania on actions carried out by the European Border and Coast Guard Agency in the Republic of Albania, ST/10302/2018/INIT, *OJ L* 46, 18.2.2019, pp. 1-2; Council Decision (EU) 2020/729 of 26 May 2020 on the conclusion of the Status Agreement between the European Union and Montenegro on actions carried out by the European Border and Coast Guard Agency in Montenegro, ST/6847/2019/REV/1, *OJ L* 173, 3.6.2020, pp. 1-2; Status Agreement between the European Union and the Republic of Serbia on actions carried out by the European Border and Coast Guard Agency in the Republic of Serbia, ST/15579/2018/REV/1, *OJ L* 202, 25.6.2020, pp. 3-15, and Agreement between the European Union and the Republic of Moldova on operational activities carried out by the European Border and Coast Guard Agency in the Republic of Moldova, ST/7204/2022/INIT, *OJ L* 91, 18.3.2022, pp. 4-21. Negotiations with North Macedonia and Bosnia and Herzegovina are about to finalise.

reported to the agency's fundamental rights officer and to the EDPS. In the future, it is envisaged that the EU will look at more distant partnerships:

‘Negotiations have concluded or are close to conclusion with Western Balkan countries, and these agreements may in the future expand beyond neighboring countries and without the territorial limitations as long as such support to third countries will contribute to the protection of the EU external borders’⁸⁴⁹.

2.4. EUAA's external relations

The European Asylum Support Office (EASO)⁸⁵⁰ was the first freedom, security and justice agency agreed under the co-decision procedure⁸⁵¹. Its establishment must be seen as a piece of a greater project conferring on the EU a shared competence on asylum for which the previous *acquis* adopted by the European Community should be revised.

Following the presentation of the European Pact on Migration and Asylum in September 2008, the European Commission advanced its Proposal to create a new regulatory agency⁸⁵² with no decision-making powers as far as asylum applications were concerned⁸⁵³. As the European Commission highlighted, the legislative harmonisation of the Member States' domestic law was not sufficient to make them converge regarding the processing of applications for international protection. As a result, the EASO would enhance 'practical cooperation' on asylum of the Member States' competent authorities and complement the reform undertaken for the CEAS⁸⁵⁴. Specifically, the agency would be in charge of:

⁸⁴⁹ Proposal for a Regulation of the European Parliament and of the Council on the European Border and Coast Guard and repealing Council Joint Action No 98/700/JHA, Regulation (EU) No 1052/2013 of the European Parliament and of the Council and Regulation (EU) No 2016/1624 of the European Parliament and of the Council. A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018, COM(2018) 631 final, Brussels, 12.9.2018.

⁸⁵⁰ Regulation (EU) 439/2010 of the European Parliament and of the Council of 19 May 2010 establishing a European Asylum Support Office, *OJ L* 132, 29.5.2010, pp. 11-28 (EASO Regulation hereinafter). The EASO Regulation was proposed on the basis of Article 63(1) and (2), as well as Article 66 of the 2002 TEC, and was finally based on Articles 74 and 78(1) and (2) TFEU.

⁸⁵¹ Daniel Warin, "Le rôle du Parlement européen dans le control des agences de l'espace de liberté, sécurité e de justice", in Cristina Blasi Casagran and Mariona Illamola Dausà, *El control de las agencias del Espacio de Libertad, Seguridad y Justicia*, Madrid, Marcial Pons, 20, pp. 11-20, p. 13.

⁸⁵² Among the different options debated there were: the maintenance of the *status quo*; the reinforcement of the competent unit of the European Commission; the creation of new networks; the establishment of a new regulatory agency (with no decision-making power); the incorporation of a supporting structure in existing agencies like the FRA, the EBCG Agency, or eu-LISA, and the establishment of a Common EU Asylum Authority with decision-making powers. Yet, the establishment of a regulatory agency was considered the best solution 'étant donné qu'elle sera la plus efficace en ce qui concerne la réalisation des objectifs, et étant donné qu'elle apparaît comme bénéficiant d'une meilleure faisabilité juridique et politique que les autres options' – see the Council of the EU, 6700/09 ADD 2, Brussels, 23 February 2009, p. 9.

⁸⁵³ Recital (14) and Article 2(6) of the EASO Regulation.

⁸⁵⁴ See the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions Policy Plan on Asylum, COM(2008) 360 final,

- developing practical cooperation between the administration in charge of examining asylum applications and the Member States by ‘facilitating the exchange of information, analyses and experience among Member States’⁸⁵⁵;
- implementing the CEAS⁸⁵⁶, and
- urgently supporting Member States under ‘particular [migratory] pressure’ with the deployment of Asylum Support Teams on the territory of the requesting Member State⁸⁵⁷.

The smart border package of 2016 proposed⁸⁵⁸ to turn the EASO into the EUAA. The new EUAA would be:

‘[...] capable of providing the necessary operational and technical assistance to Member States, increasing practical cooperation and information exchange among Member States, supporting a sustainable and fair distribution of applications for international protection, monitoring and assessing the implementation of the CEAS and the capacity of asylum and reception systems in Member States, and enabling convergence in the assessment of applications for international protection across the Union’⁸⁵⁹.

The lack of political agreement on the 2016 asylum package⁸⁶⁰ slowed down the adoption of the EUAA Proposal and in 2018 the European Commission decided to amend it⁸⁶¹. The amended Proposal aimed at aligning the EUAA regime with the new empowerment conferred on the EBCG Agency in 2018 and in light of the Proposal of a new Directive on return. The

Brussels, 17.6.2008, and the Green Paper on the future Common European Asylum System, COM(2007) 301 final, Brussels, 6.6.2007.

⁸⁵⁵ See Articles 3 to 6 of the EASO Regulation contemplating: the exchange of information regarding the identification and pooling of best practices in asylum matters; the promotion and coordination of activities relating to information on countries of origin; the supporting of relocation within the EU with the agreement of both the Member States concerned and the beneficiary of international protection, and the support of trainings in national administrations, courts and tribunals, as well as national services responsible for asylum matters in the Member States.

⁸⁵⁶ See the Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Asylum and repealing Regulation (EU) No 439/2010, COM(2016)0271 final – (2016)0131 (COD), Brussels, 4.5.2016.

⁸⁵⁷ See Article 2(2) of the EASO Regulation. According to its Article 8, a ‘particular pressure’ is caused by ‘heavy and urgent demands on their reception facilities and asylum systems’ and may be characterised by ‘sudden arrival of a large number of third-country nationals who may be in need of international protection and may arise from the geographical or demographical situation of the Member States’.

⁸⁵⁸ Proposal for a Regulation of the European Parliament and of the Council, COM(2016)0271 final, Brussels, 4.5.2016. The Proposal is underpinned by Article 78(1) and (2) TFEU only.

⁸⁵⁹ Proposal for a Regulation of the European Parliament and of the Council, COM(2016) 271 final, Brussels, 4.5.2016.

⁸⁶⁰ See for example the Italian’s position rejecting any control mechanism by the EASO as a sort of pre-infringement procedure enacted by the Commission in Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Asylum and repealing Regulation (EU) No. 439/2010*, 10517/16, Brussels, 6 October 2016, p. 35.

⁸⁶¹ Council of the EU, *Amended proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Asylum and repealing Regulation (EU) No. 439/2010 - A contribution from the European Commission to the Leaders’ meeting in Salzburg on 19-20 September 2018*, 12112/18, Brussels, 13 September 2018.

European Commission suggested that the EUAA was a ‘tangible example of European solidarity’ with enhanced cooperation with the EBCG Agency to coordinate the procedure of international protection with those of return⁸⁶². The EUAA Regulation was adopted in December 2021⁸⁶³ and it equips the EUAA with liaison officers that may be deployed in the Member States to⁸⁶⁴:

- act as an interface between the agency and Member States’ authorities responsible for asylum and immigration and other relevant services;
- support the collection of information required by the agency;
- contribute to promoting the application of Union law on asylum, including with regard to the respect of fundamental rights;
- where requested, assist the Member States in preparing their contingency planning regarding measures to be taken in order to deal with possible disproportionate pressure on their asylum and reception systems;
- facilitate the communication between Member States and between the Member State concerned and the agency;
- share relevant information from the agency with the Member State concerned, including information about ongoing assistance, and
- regularly report to the Executive Director on the asylum situation in the Member State concerned and its capacity to manage its asylum and reception systems effectively.

⁸⁶² The European Commission advanced the following reforms: Article 16 on operational and technical assistance for which the EUAA could

‘[...] prepare decisions on applications for international protection and provide those decisions to the national competent authorities who will then take the decision on the individual applications and have full responsibility for processing this request. The Agency would also be able to support Member States with handling their appeals in asylum cases by, among others, performing legal research, producing reports and analysis and providing other legal support at the request of the courts or tribunals with full respect of judicial independence and impartiality’.

Article 21 on migration management support teams to deploy in the absence of disproportionate migratory challenges too; Article 16a on enhanced assistance with the procedure for international protection and the Dublin procedure, and Article 47 regards the appointment of the Deputy Executive Director for which purpose the European Commission suggested that the list of candidates for a deputy Executive Director to the Agency’s Management Board should be submitted by the Commission instead of the Executive Director.

⁸⁶³ See the “Accord entre le Parlement européen et la Présidence du Conseil de l’UE sur la nouvelle Agence européenne de l’asile”, *Bulletin Quotidien Europe*, No. 12751, Brussels, 29.06.2021, and the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Asylum and repealing Regulation (EU) No. 439/2010 (First reading) – Letter to the Chair of the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE)*, 10352/21, Brussels, 30 June 2021, confirming that a political agreement in the trilogue formation was reached on the 29 June 2021. The new EUAA Regulation will enter into force on the 31 December 2023.

⁸⁶⁴ *Ibid.*, p. 35.

2.4.1. The processing of personal data by the EUAA

With the new Regulation, the exchange and analysis of information became one of the five goals the EUAA is in charge of⁸⁶⁵ and a duty was imposed on Member States to cooperate with the agency and an obligation to exchange information with it⁸⁶⁶. The EUAA is allowed to process personal data for the performance of its tasks that are usually classified as permanent, special, and urgent types of support. Specifically, the EUAA may:

- provide operational and technical assistance to Member States;
- carry out case sampling for the purposes of the monitoring exercise, possibly handling applications for international protection for children or vulnerable persons;
- facilitate the exchange of information with Member States, the EBCG Agency, Europol and Eurojust, and
- analyse information on asylum trends for administrative purposes⁸⁶⁷.

First of all, the EUAA supports the Member States in implementing the asylum *acquis* – this is also referred to as ‘permanent support’ in the EUAA programs – through trainings and the exchange of best practices among the Member States. In addition, the new EUAA is able to independently gather and to analyse information in the EU and in third countries and, specifically, to draft situational reports on third countries of origin. The gathering and analysis of information on third countries of origin is directed at keeping the list of ‘safe countries of origin, third countries designated as safe countries of origin or safe third countries or to which the concepts of safe third country, first country of asylum or European safe third country by Member States apply’ updated⁸⁶⁸. In these terms, the EUAA can identify, collect, and analyse information relating to the structures and staff – especially for translation and interpreting – available in countries of origin and relating to the support the agency hands and manages of asylum cases. The EUAA can use existing arrangements and, in case of publicly accessible information, it can process personal data related to:

- the processing of applications for international protection by national administration and authorities, and
- national and legal developments in the field of asylum, including case law databases.

⁸⁶⁵ Article 2(1)(b), (e), and (h), of the EUAA Regulation.

⁸⁶⁶ Article 4(5) of the EUAA Regulation.

⁸⁶⁷ Article 29 ff. of the EUAA Regulation.

⁸⁶⁸ Recital (10) and Article 9 of the EUAA Regulation.

In order to facilitate the exchange of information on countries of origin among Member States, the European Commission proposed to turn the European readmission agreements system into a ‘fully-fledged EU country of origins database [...] to support practical cooperation in the field of asylum’⁸⁶⁹ alongside the databases of each Member State⁸⁷⁰. The EUAA may create factual, legal, and case law databases on the application and interpretation of Union, national, and international asylum instruments making use, in particular, of existing arrangements⁸⁷¹. One of the projects launched by the agency in its work program⁸⁷² consisted of the establishment of a database of national jurisprudence to be shared among Member States based on Article 33 of the Dublin II Regulation⁸⁷³. Yet, these databases must not process personal data unless it has been obtained by the agency from publicly accessible documents⁸⁷⁴. In broader terms, the EUAA is supposed to develop, in cooperation with eu-LISA, its own information system to exchange classified information⁸⁷⁵ for which the EDPS warned that it must also to adopt high security measures⁸⁷⁶.

Since 2012, the EUAA has been working on the elaboration of a tailor-made Early Warning and a Preparedness System on asylum⁸⁷⁷ – also known as ‘special support’ – that aims at enhancing reception systems and fostering capacity building in Member States that require support. In 2012, for example, the EUAA gave special support to Italy to implement the asylum package adopted by the EU in 2011-2013. In the Commission Staff Working Document specific concerns were raised with regard to Malta and Greece’s flow of immigrants⁸⁷⁸. The Early Warning and Preparedness System is based on statistical data in a similar manner to the EBCG Agency vulnerability assessment for which the two agencies are supposed to synergise, given the need to evaluate the external pressure the EU might be called upon to face⁸⁷⁹. The EUAA

⁸⁶⁹ Council of EU, 6700/09 ADD 1, Brussels, 23 February 2009, p. 73.

⁸⁷⁰ See the Council of the EU, *Commission Staff Working Document on the internal Evaluation of the European Asylum Support Office (EASO)*, 8471/14, Brussels, 2 April 2014, p. 12.

⁸⁷¹ Article 6(3) of the EUAA Regulation.

⁸⁷² Council of the EU, *EASO Work Programme 2014*, 14377/13, Brussels, 7 October 2013, p. 25.

⁸⁷³ Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, *OJ L* 50, 25.2.2003, pp. 1-10.

⁸⁷⁴ Recital (11) of the EUAA Regulation.

⁸⁷⁵ Article 29(2) of the EUAA Regulation.

⁸⁷⁶ See the Opinion of the EDPS No. 07/2016 on *the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations)*, Brussels, 21.09.2016, p. 17.

⁸⁷⁷ See the Council of the EU, *EASO Work Programme 2013*, 14372/12, Brussels, 2 October 2012, p. 5.

⁸⁷⁸ See the Council of the EU, 6700/09 ADD 1, Brussels, 23 February 2009, p. 11 ff., and the Council of the EU, *Greece’s National Action Plan on Asylum Reform and Migration Management = information by Greece, the Commission, Frontex and EASO*, 15358/12, Brussels, 23 October 2012.

⁸⁷⁹ See *infra*.

cooperates with the EBCG Agency to manage ‘Migration Management Support Teams’ deployed by the EUAA to Member States facing pressure or to the hotspots according to the 2016 EBCG Agency Regulation⁸⁸⁰. These teams are coordinated by the EBCG Agency and aim to:

- screen third-country nationals, including managing their identification, registration, and where requested by Member States, their fingerprinting;
- register applications for international protection and, where requested by Member States, examine such applications; and
- provide information on asylum procedures, including relocation and specific assistance to applicants or potential applicants that could be subject to relocation.

The EUAA can provide ‘emergency support’ by deploying asylum support teams in an emergency situation characterised by a ‘particular pressure’ following the request of the Member State concerned, this is perceived as a ‘tangible’ expression of the principle of solidarity among Member States, also known as intra-EU solidarity⁸⁸¹, set forth in Article 80 TFEU. These teams are made up of authorities selected from both an asylum intervention pool and a national pool that gathers together the agency's staff, staff from the Member States and/or experts seconded by Member States to the agency. During the negotiations of the EUAA Regulation the Council limited the empowerment of the asylum support teams, resulting in the EUAA only having responsibility for:

‘[...] analysing data on any sudden arrival of large numbers of third-country nationals which may put particular pressure on asylum and reception systems and for ensuring that relevant information is exchanged rapidly between Member States and the Commission, including through the use of existing early warning systems or, if necessary, the Office's own system established for this purpose’⁸⁸².

For the deployment of an asylum support team, the EUAA Regulation foresees that the Executive Director must agree on an operating plan. Such a plan may establish the databases that the teams are authorised to consult, as well as the equipment they may carry in the requesting Member State. The aim of the asylum intervention pool is to have a database of

⁸⁸⁰ See Article 16(1)(c) of the EUAA Regulation, and Articles 18 and 19 of the 2016 EBCG Agency Regulation.

⁸⁸¹ See the Council of the EU, *Council Conclusions on a Common Framework for genuine and practical solidarity towards Member States facing particular pressure on their asylum systems, including though mixed migration flows*, 3151 Justice and Home Affairs Council meeting Brussels, 8 March 2012, and the EU Action on Migratory Pressures - A Strategic Response, 9650/12, Brussels, 10 May 2012. Unfortunately, with scarce results as the failure of the asylum relocation programme EUREMA testifies – see the Council of the EU, 8471/14, Brussels, 2 April 2014, p. 29 ff.

⁸⁸² Council of the EU, *Position en première lecture adoptée par le Conseil le 25 février 2010 en vue de l'adoption du règlement du Parlement européen et du Conseil portant création d'un Bureau européen d'appui en matière d'asile = Exposé des motifs du Conseil*, 16626/2/09 REV 2 ADD 1, Brussels, 25 February 2010, p. 4.

experts who shall be made available by EU Member States for deployment when a situation of particular pressure arises⁸⁸³. During these operations, the EUAA will collect ‘operational data’ directly from the Member States in order to undertake the practical cooperation it will facilitate and in order to produce reliable statistics in a similar manner to that of the EBCG Agency’s Risk Analysis Network. The asylum support teams are furnished with experts for the ‘[...] identification and registration of third countries nationals, interpreting services, information on countries of origin and knowledge of the handling and management of asylum cases, as well as by assisting national authorities competent for the examination of applications for international protection and by assisting with relocation’⁸⁸⁴. In these terms, the EUAA is entitled to assist Member States in the identification and registration of third country-nationals⁸⁸⁵ where the Asylum Support Teams are deployed.

The categories of data to be collected or transmitted by the Member States or by the EUAA as part of the ‘operational and technical assistance’ were initially limited to the name, date of birth, gender, nationality, profession or education, fingerprints, and digitised photograph of third-country nationals⁸⁸⁶; however, the negotiations have progressively expanded this list also to include, for example, data concerning the health or specific vulnerabilities of a third-country national⁸⁸⁷. In cases resettlement, for example, the EUAA is enabled to process different types of data including: the full name, date and place of birth, place of residence or stay, gender, age, nationality, profession, education, family, date and place of arrival, fingerprints, and facial image data of a third-country national, and the status of a third-country national in relation to international protection⁸⁸⁸. The EUAA Regulation specifies that in no case can the data can be stored for more than thirty days, unless it is processed for ‘administrative purposes’⁸⁸⁹, thus inserting once again a distinction between ‘operational’ and ‘administrative’ personal data. In this regard, the European Commission Staff Document makes clear that, although they are third country nationals, asylum seekers benefit from the CFREU’s rights and freedoms and, consequently, they are entitled to the right to the protection of personal data⁸⁹⁰.

⁸⁸³ See the Council of the EU, 14372/12, Brussels, 2 October 2012, p. 24.

⁸⁸⁴ Recital (26) of the EUAA Regulation.

⁸⁸⁵ Article 16(2)(a) of the EUAA Regulation.

⁸⁸⁶ Article 32 of the EUAA Regulation.

⁸⁸⁷ Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Asylum and repealing Regulation (EU) No. 439/2010 – State of play and guidance for further work*, 9563/17, Brussels, 29 May 2017, p. 227.

⁸⁸⁸ Article 32 of the EUAA Regulation.

⁸⁸⁹ Recital (40) of the EUAA Regulation.

⁸⁹⁰ Council of the EU, 6700/09 ADD 1, Brussels, 23 February 2009, p. 52 ff.

As part of its operational activity, the EUAA is granted access not only to Member States' databases, but also to the European ones⁸⁹¹. It is not clear in which terms the EUAA may be granted access to the large-scale IT systems and the interoperability components via the national interfaces. We should warn that no regulation provides database access to the EUAA staff and, if in practice they do access them (including indirectly), legal coverage would be needed. Access rights are laid down in (unpublished) operational plans that bind the agency, the host, and the participating Member States. In case of the transmission of data to the EBCG Agency, this must be deleted after the transmission, but may be re-used for information analysis on the asylum situation in the Member State⁸⁹². The maximum period of storage is three months.

Given that personal data could be processed by EU as well as Member States' staff in the territory of one or more Member State, the EDPS complained about the lack of a clear determination of who is accountable for the processing of personal data and suggested that Member States be designated as data controllers. The EUAA Regulation clarifies that three different data protection regimes may apply to the EUAA's activities: the EUDPR for the EUAA staff; the GDPR, and the LED for the Member States' authorities depending on the purpose of the personal data processing⁸⁹³. Specifically, when the processing of personal data is carried out by experts from the asylum support teams under the instruction of the host Member State and when the teams are providing operational and technical assistance to that Member State, the GDPR should be applicable⁸⁹⁴. However, the co-presence of both Union staff and Member States' authorities suggested that opting for the designation of 'joint controllers' would distribute the responsibility for data protection processing activities. The fact that EUAA Regulation specifies that third country nationals must be informed of the data processing activity at the time of the collection of their personal data according to Article 13 GDPR as well as of 'details of the relevant national supervisory authority responsible for monitoring and enforcing compliance with Regulation (EU) 2016/679'⁸⁹⁵ is welcomed. In addition, the need for a Data Protection Officer and a Fundamental Rights Officer⁸⁹⁶ has been established within the EUAA, which will lay down in a MoU the respective responsibility in case of complaints.

⁸⁹¹ Article 28(4) of the EUAA Regulation.

⁸⁹² See the Opinion of the EDPS No. 07/2016 on *the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations)*, Brussels, 21.09.2016, p. 16.

⁸⁹³ Council of the EU, 10352/21, Brussels, 30 June 2021, p. 24.

⁸⁹⁴ Council of the EU, 9563/17, Brussels, 29 May 2017, p. 219.

⁸⁹⁵ *Ibid.*, p. 230.

⁸⁹⁶ Council of the EU, 10352/21, Brussels, 30 June 2021, pp. 81 ff.

2.4.2. The EUAA's working arrangements

The EUAA is mandated to support the external dimension of the CEAS⁸⁹⁷ that foresees both the improvement of the resettlement and Regional Protection Programmes⁸⁹⁸ and the enhancement of third countries' system of protection⁸⁹⁹ through the exchange of information and other actions directed at implementing instruments and mechanisms relating to the external dimension of the CEAS⁹⁰⁰.

The EUAA is supposed to seal a close cooperation relationship with competent authorities established in third countries, international organisations competent in matters covered by its founding instrument, and third countries as part of the working arrangements it concludes and 'in accordance with the Union's external policy'⁹⁰¹. While still called EASO, the agency took part in the meetings around the EU Mobility Partnership with Tunisia and Morocco, the EU-Jordan Dialogue on Migration, Mobility and Security, as well as to the Budapest process⁹⁰². As a result, and although the EUAA was granted legal personality in order to conclude a headquarter agreement⁹⁰³, it is not allowed to conclude international agreements. In any case,

⁸⁹⁷ Article 1(2) of the EUAA Regulation. We will not here address the EUAA's intra-institutional relations, though we must recall that the agency cooperates with the EBCG Agency, the FRA, Europol, Eurojust, CEPOL, European Monitoring Centre for Drugs and Drug Addiction, OLAF, and other bodies like the European Migration Network according to Article 32(2)(b) and 32(4) of the EUAA Regulation. So far, the EUAA website published working arrangements with FRA, EBCG Agency, and eu-LISA. The EUAA-FRA working arrangement, for example, provides for the exchange of information as far as the cooperation with third countries and international organisations is concerned, and in the frame of research activities of common interests. The EUAA-EBCG Agency working arrangement is not published but from the EASO-EBCG Agency cooperation plan, 18 July 2019, available at www.easo.europa.eu, it is understandable that this arrangement follows the structure of the one concluded with the FRA and concretely, that it covers four layers of cooperation: first, operational cooperation; second, information and analysis; third, capacity building and, fourth, horizontal cooperation. Second, in the frame of information and analysis cooperation, the agencies collaborate for the elaboration a Common Situational Picture on irregular migration and persons in need of international protection that includes the interoperability of authorisation and integration of the EUAA Information and Documentation System and the Frontex Integrated Return Management Application platforms, as per Service Legal Agreement. Together with Europol, the two agencies are required to elaborate joint analyses for obtaining a joint intelligence picture on secondary movements of irregular migrants and asylum seekers across the Schengen area. Also, the agencies agree to cooperate in the elaboration of the EBCG Agency's Vulnerability Assessment and in the procurement of external expertise on countries of origin and transit for the preparation of Country Intelligence Reports.

⁸⁹⁸ Resettlement consists in the 'transfer of refugees from a third country in which they have sought asylum to an EU State that has agreed to grant them permanent protection there' while Regional Protection Programmes, instead, 'were developed under the Programme for Freedom, Security and Justice for the years 2005 to 2010. They aim to enhance the protection capacity of the regions involved and provide Durable Solutions' – see the Council of the EU, 6700/09 ADD 1, Brussels, 23 February 2009, p. 13 ff.

⁸⁹⁹ See the table available in the Council of the EU, 6700/09 ADD 2, Brussels, 23 February 2009, p. 5.

⁹⁰⁰ Article 35(2) of the EUAA Regulation.

⁹⁰¹ Recital (38) of the EUAA Regulation.

⁹⁰² Council of the EU, *EASO Annual Report 2012*, 13455/13, Brussels, 17 September 2013, p. 19.

⁹⁰³ Article 68 of the EUAA Regulation.

even if the EUAA can conclude working arrangements⁹⁰⁴ with partners that have not already committed to the EU, the agency is forbidden to create an independent external policy⁹⁰⁵.

The new EUAA Regulation sets forth that the agency is in charge not only of coordinating the exchange of information, but also operational cooperation between the Member States and third countries, and it can host third countries' officials as observers of its operational activity⁹⁰⁶. The EUAA can deploy liaison officers in the Member States as well as in third countries⁹⁰⁷ for establishing and maintaining contacts with the competent authorities of the third country to which they are assigned with a view to gathering information and contributing to the establishment of protection-sensitive migration management and, as appropriate, to facilitating access to legal pathways to the Union for persons in need of protection, including through resettlement. The liaison officers shall coordinate closely with Union delegations as well as international organisations and bodies, in particular UNHCR, where appropriate⁹⁰⁸. The deployment of liaison officers in third countries of origin and transit must be subjected to the Management Board's approval while the European Parliament must be kept informed⁹⁰⁹. Moreover, the EUAA may organise training activities in cooperation with Member States or third countries in their territory⁹¹⁰. The EUAA must coordinate the exchange of information in cases of resettlement⁹¹¹, and it should enable the implementation of international agreements concluded with third countries⁹¹².

With the new EUAA Regulation, the agency has been mandated the ability to conclude working arrangements with third countries⁹¹³ that are ultimately subjected to the European Commission's approval, while the European Parliament and the Council are informed before their conclusion⁹¹⁴. This cooperation must respect norms and standards equivalent to those of the EU, if the cooperation is exercised in the territory of the third country⁹¹⁵. The EUAA may

⁹⁰⁴ Among those that have concluded agreements with the EU, the EUAA Regulation refers to Iceland, Liechtenstein, Norway and Switzerland – Article 34 of the EUAA Regulation.

⁹⁰⁵ Recital (38) of the EUAA Regulation: 'It does not, under any circumstances, fall within the mandate of the Agency to formulate independent external policy'.

⁹⁰⁶ Articles 1(2) and 36 of the EUAA Regulation.

⁹⁰⁷ Article 36 of the EUAA Regulation.

⁹⁰⁸ Article 36(3) of the EUAA Regulation *in fine*.

⁹⁰⁹ Article 36(2) and (4) of the EUAA Regulation.

⁹¹⁰ Article 7(8) of the EUAA Regulation.

⁹¹¹ Article 35(3) of the EUAA Regulation.

⁹¹² Article 35(4) and (5) of the EUAA Regulation.

⁹¹³ Article 35 of the EUAA Regulation.

⁹¹⁴ Some Member States, like Italy, insisted on involving the Council too – see the Council of the EU, 10517/16, Brussels, 6 October 2016, p. 61.

⁹¹⁵ See recital (24) and Article 35 of the EUAA Regulation.

support a Member State in the implementation of resettlement as part of its cooperation with third countries⁹¹⁶. Also, the agency shall participate in the implementation of international agreements concluded by the Union with third countries regarding matters covered by mandate⁹¹⁷. Although the European Commission's Proposal initially excluded any type of transfer of personal data to third parties⁹¹⁸, the EUAA Regulation foresees derogations that include cases of cooperation with third countries for the purposes of resettling third country nationals⁹¹⁹.

The EUAA has always collaborated with the UNHCR⁹²⁰ due to its consolidated expertise in the human rights field. Such a strong relationship includes the possibility of the UNHCR participating in the Management Board of the agency as an observer, the guidelines for which are taken into account by the EUAA, and the establishment of UNHCR liaison officers in the EASO's headquarters, in Malta. The EUAA and the UNHCR can agree *ad hoc* projects as was done, for example, in Greece to foster the administrative appeals instance of asylum seekers⁹²¹. From the EUAA's activity report⁹²², it is clear that the EUAA also engaged in relations with: the Council of Europe, the General Directors of Immigration Service Conference, the Inter-Governmental Consultations on Migration, and the IOM. For our research, the working arrangements with UNHCR and IOM are especially relevant⁹²³.

The EUAA-UNHCR working arrangement of 13 December 2013⁹²⁴ is based on a list of shared principles and values that finds as its points of reference the 1951 Geneva Convention and the EU asylum *acquis* based on the wider concept of international protection. The arrangement provides for different types of support. Firstly, the so-called permanent support⁹²⁵ includes the execution of trainings, the exchange of countries of origin, and the exchange of

⁹¹⁶ Article 35(3) of the EUAA Regulation.

⁹¹⁷ Article 35(4) of the EUAA Regulation.

⁹¹⁸ Article 30(4) of the EUAA Regulation: 'The transfer of personal data processed by the Agency and the onward transfer by Member States to authorities of third countries or third parties, including international organisations, of personal data processed in the framework of this Regulation shall be prohibited'.

⁹¹⁹ Article 30(5) of the EUAA Regulation and the Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Asylum and repealing Regulation (EU) No. 439/2010*, 12701/16, Brussels, 5 October 2016, p. 49.

⁹²⁰ See Article 38 of the EUAA Regulation.

⁹²¹ See the Council of the EU, 13455/13, Brussels, 17 September 2013, p. 16.

⁹²² See the Council of the EU, 14372/12, Brussels, 2 October 2012, p. 31.

⁹²³ See Julinda Beqiraj, Jean-Pierre Gauci, and Anna Khalfaoui, *loc. cit.*

⁹²⁴ EUAA-UNHCR working arrangement, 13 December 2013, available at www.easo.europa.eu. Note that Article 50 of the EASO Regulations set forth that the (then) EASO-UNHCR working arrangement should have been adopted by the Management Board while Article 30 of the EUAA Regulation has also imposed the obligation to inform the European Parliament and the Council.

⁹²⁵ Articles 3-7 of the EUAA-UNHCR working arrangement of 21 July 2021.

best practices on: quality activities, interpretation and the list of available languages, and on information and expertise related to the identification, protection, and needs of vulnerable persons. Secondly, the arrangement provides for special support⁹²⁶ addressed to specific Member States' needs which may imply the creation of tailor-made activities on a case-by-case basis. In addition, special support also covers intra-EU relocation between Member States. Thirdly, emergency support can be enacted through the deployment of experts selected from their respective pools⁹²⁷ and consists of the exchange of information on Member States' needs for which purpose the EUAA and the UNHCR may support reciprocal initiatives on a case-by-case basis. Specific forms of support are also envisaged for:

- the gathering and analysis of information⁹²⁸ in order to prepare situational reports and to cooperate in early warning, preparedness, and crisis management;
- the enhancement of cooperation with associate and other third countries and international organisations, including on resettlement⁹²⁹, and
- a general horizontal cooperation in matters of common interest⁹³⁰.

The final rules⁹³¹ provide, among others, for: the establishment of contact points facilitating the exchange of information on the implementation of the arrangement; resolve disputes through consultations and negotiations or through the arbitration clause agreed in the Financial and Administrative Framework Agreement between the UN and the EU; the provision of liability of each agency for the activity of its own staff, personnel or subcontractors; the possibility to amend and supplement the arrangement, the safeguarding of privileges and immunities, and its entry into force.

On 21 July 2021, the EUAA and the UNHCR signed a new working arrangement⁹³² to update their reciprocal cooperation according to their respective fields of competences. Among the principles listed in its Article 2, a reference to the 'dissemination and data protection rules and policies' has been inserted as far as the exchange of relevant information, documents, and other material is concerned. In addition, a new provision has been inserted regarding cooperation on protection-related tools and guidance that enables the parties to invite each other to network meetings. Also, the parties agreed to inform each other before the publication of country-

⁹²⁶ Articles 8 and 9 of the EUAA-UNHCR working arrangement 21 July 2021.

⁹²⁷ Articles 10 and 11 of the EUAA-UNHCR working arrangement 21 July 2021.

⁹²⁸ Article 12 of the EUAA-UNHCR working arrangement 21 July 2021.

⁹²⁹ Articles 13 and 14 of the EUAA-UNHCR working arrangement 21 July 2021.

⁹³⁰ Articles 15-20 of the EUAA-UNHCR working arrangement 21 July 2021.

⁹³¹ Articles 21-28 of the EUAA-UNHCR working arrangement 21 July 2021.

⁹³² Second EUAA-UNHCR working arrangement of 21 June 2021.

specific guidance so as to provide input to one another. As far as vulnerable persons are concerned, a specific reference to stateless persons was inserted. The Articles regulating special support have been laid down in greater detail than before in order to avoid duplication of efforts and to better coordinate their mandate. Emergency support is now labelled as ‘Contingency Planning and Emergency Operations’ since it is foreseeable that both contingency and preparedness plans will be jointly developed. As for the cooperation in the data and information gathering and analysis field, the parties agreed to exchange information regarding good practices on methodologies and tools for collecting testimonies directly from applicants for, and beneficiaries of, international protection ‘based on the relevant legal structures governing data protection’. Moreover, another new provision was inserted to enhance the cooperation of the parties on the elaboration of the EUAA situation of asylum in the EU Annual Report, as well as of the publicly available sources, tools, and platforms feeding the information gathering process, such as asylum and reception information platforms, case law databases, asylum legislation and policy databases. Also, the norms dedicated to the external dimension of their cooperation have been widened: Article 15 specifies that collaboration in the enhancement of capacity-building activities may consist, *inter alia*, of the ‘development and improvement of case management systems, accelerating and streamlining procedures/workflows, backlog prevention/reduction, quality assurance, assessments and/or determinations of the best interests of the child and reception conditions, where relevant and appropriate’. In addition, the EUAA and the UNHCR are supposed to consult and coordinate in the provision or planned provision of capacity-building support, as well as the deployment of relevant programming in third countries, which is channelled through cooperation between the EUAA’s Third Country Cooperation Network and the Asylum Support Group established by the UN Global Compact on Refugees. The provision on resettlement cooperation has been enriched by a reference to ‘Humanitarian Admission and Complementary Pathways’, though no specification is given regarding their added value. The new arrangement specifies that cooperation between the two parties must be channelled through the so-called institutional focal points and that these are located in the UNHCR’s liaison office to the EUAA in Malta, and in the EUAA’s European and International Cooperation Unit.

Among the other organisations with which the EUAA has sealed an arrangement, the IOM⁹³³ stands out. First of all, the arrangement set forth norms on general principles that summarise the field of cooperation agreed between the parties, which includes: the participation of the

⁹³³ EUAA-IOM working arrangement of 22 July 2019.

IOM in the EUAA network meetings, and the parties agreed reciprocal participation in their respective meetings through the sending of representatives; quarterly meetings between the EUAA headquarters and the IOM Regional Offices for the European Economic Area, the EU and the North Atlantic Treaty Organisation for the implementation of the arrangement; the appointment of institutional focal points by both parties, and ‘appropriate measures by [EUAA] and IOM’ to ensure effective cooperation and liaison between the two parties. The fields of cooperation are included in Article VI of the arrangement and include: early warning, preparedness and contingency planning; asylum and reception of applicants for international protection; returns; durable solutions including resettlement and other legal pathways; the provision of support to migrants in vulnerable situations and/or with specific protection needs; training activities, and capacity building activities. The exchange of data, information and documentation is regulated by Article IV that includes: displaced populations in regions of origin, populations in transit, resettlement, humanitarian admission, relocation, family reunification, the IOM displacement tracking matrix, returns – including assisted voluntary return and reintegration –, reception, social media monitoring, private and community based sponsorship schemes and others, both within the EU Member States and the third countries concerned. In its fourth paragraph, it is specified that: ‘Any data sharing shall be in line with the respective mandate of the Parties, and without prejudice to principles and rules on the protection of personal data, sharing rules, and confidentiality levels established by the respective Parties (and original data owners, in case of Member States’ data for example)’.

The implementation of the working arrangement takes place through a variety of approaches: work programs; representation; the possibility to adopt plans and roadmaps; an annual meeting at the senior management level, and the participation of the IOM Consultative Forum. Final provisions concern the confidentiality of the shared information; intellectual propriety rights; privileges and immunities; dispute settlement resolution through consultations and negotiations; entry into force; amendments and duration, and the potential revise of the working arrangement following the ‘adoption’ of the EUAA amended Proposal Regulation. The provision of working arrangements by which personal data can flow out of the EU is not new, as our study on the EBCG Agency shows. In fact, the GDPR and the DPREU legitimise such agreements with the approval of the competent national authority or the EDPS respectively⁹³⁴. However, we wonder at this point of our research whether these framework instruments should be amended, as their non-enforceability raises doubts as to whether they can be challenged in

⁹³⁴ See Chapter IV.

court. As a last resort, their soft nature leaves an aura of uncertainty as to whether the data subject's fundamental right to protection of personal data is actually respected.

CONCLUSIONS

Our investigation started by pointing out that, in May 2019, the EU adopted a framework regarding the interoperability among the EU large-scale IT systems in the field of borders, visas, police and criminal judicial cooperation, asylum, and migration. Regulations (EU) 2019/817 and 2019/818 aim at interconnecting the six EU large-scale IT systems, that currently exist or are soon to be implemented within the AFSJ under the auspices of a new architecture that supports their functioning. These systems are: the SIS; the VIS; the EES; the ETIAS; the Eurodac, and the ECRIS-TCN. Interoperability is defined as the ability of systems to communicate, exchange data, and use the information previously stored in centralised, shared “databases”. Yet, we warned that the highly technical language used by the co-legislators has led to harsh criticism questioning the extent of its reach.

Stretching across different legal systems, interoperability enables information and personal data to flow throughout different jurisdictions, even though diverse cultural and juridical approaches to privacy are in place, as it preserves key elements of diversity. Thus, we presented “legal interoperability” as an alternative to normative harmonisation, enabling the compatibility of different legal systems, without the need to encounter domestic legislations. Specifically, interoperability among different jurisdictions – or “global” interoperability – is based not on a common framework in the human rights field, but on the principles of mutual recognition and enforcement cooperation: the former is founded on the assumption that other legal systems comply with common values surrounding privacy and personal data protection; the latter requires the body responsible for the processing activity to demonstrate its accountability.

We urged that, in the EU context, transferring personal data without counting on harmonised normative standards hampers the guarantees set forth under the Union legislation on the protection of personal data which ordinarily requires a third country or international organisation to apply a level of protection “equivalent” to that of the EU. The human right to “privacy”, in its multifaced conceptualisations, and the right to the protection of personal data firstly consecrated in Article 8 of the CFREU, are undermined when the disclosure of information regarding an individual leads to disproportionate interferences with said individual. After the Snowden scandal, legal systems previously considered to be close to the European model must be looked at with suspicion, as they have proved to be incompatible with the EU hierarchy of values. Consequently, “global interoperability” has to be carefully balanced with the individuals’ rights to privacy and to the protection of personal data.

According to Article 50 of the sister Regulations, the communication of personal data to third countries, international organisations and private parties is regulated by the underlying large-scale IT systems and Union agencies' regimes on the transfer of personal data. In addition, the IO Regulations advance a forthcoming agreement with Interpol which would interconnect interoperability with SLTD and TDAWN databases. The co-legislators presented the interoperability framework as an efficient and effective solution to achieve freedom, security, and justice objectives. Indeed, the rules underlying the communication of personal data echo those established by the EU in its data protection *acquis*, namely: Chapter V of the GDPR; Chapter V of the LED, and Chapter V of the EUDPR. However, prior to our pre-doctoral research it was not clear whether, and under what terms, the external dimension of interoperability manages to respect the normative parameters set forth in international and EU law. As a result, we wondered whether the rules and principles applied by the EU to the communication of personal data to third parties in its external relations are being respected, circumvented, or breached.

The pre-doctoral study aimed at determining the external reach of the interoperability framework established under Regulations (EU) 2019/817 and 2019/818, that is, its reach beyond the EU's external borders. Thus, this dissertation assessed whether the interoperability of centralised Union systems and components with foreign databases is lawful and sustainable – i.e., consistent – *vis-à-vis* the rules and principles that underpin the EU external action. Specifically, we analysed whether Article 50 of the IO Regulations complies with the international and supranational legal frameworks and, if so, whether the individuals' rights, especially the fundamental right to the protection of personal data, are truly guaranteed.

1. The EU's personal data protection *acquis* within the AFSJ

1.1. Before the international community's delayed, soft response to the protection of the human right to privacy in the new digital environment, the EU was given an express competence regarding the protection of personal data and the free movement of such data in 2007 (Article 16 TFEU). This legal basis granted it a leading role in the elaboration and worldwide promotion of principles on the protection of personal data.

During the XXI century, the technological revolution quickly showed that the human right to privacy, which had been already consecrated in universal international instruments – i.e., Article 12 of the UDHR and Article 17 of the ICCPR – needed to be reinterpreted to safeguard the dignity of human beings in the new digital environment. Given that this right can be

perceived differently depending on the cultural and juridical environment of the individual, with Convention 108 the Council of Europe managed to do little more than to establish a framework of principles to protect individuals with regard to the automatic processing of personal data. Since 1981, Convention 108 has been the main point of reference to protect the individual from the misuse of new technologies until a specific competence was conferred upon the EU that would enable it to adopt its own data protection *acquis*.

The EU *acquis* on the protection of personal data originates from the positive integrationist logic of removing obstacles to the exchange of personal data among the Member States caused by their diverging legislations. In the lack of an express conferred competence in the founding Treaties, the European Community adopted its own data protection legislation based on the harmonisation clause – currently Article 114 TFEU – although not all its Member States had legislated on the matter. The DPD laid down minimum rules on the protection of personal data and on the free movement of such data, some of which are codified in the CFREU. Additional data protection principles – such as that on security, integrity, and confidentiality – instead, have been consolidated by the CJEU’s case law. The intergovernmental framework characterising PJCCM policies legitimised the adoption of an *ad hoc* regime set down in the DPF, which the Member States preserved after the entry into force of the Lisbon Treaty. In 2007, a new Article was inserted into the TFEU and, as a matter of course, within the dispositions of general application conferring on the EU a cross-cutting competence on the protection of personal data and the free movement of such data, with the sole exception of the CFSP that relies upon Article 39 of the TEU.

1.2. Article 16 TFEU confers on the EU a new competence on the protection of personal data and on the free movement of such data, the exercise of which must follow the principles of pre-emption, subsidiarity and proportionality. These principles must be read in the light of the fundamental right to the protection of personal data enshrined in Article 8 of the CFREU.

The provision of Article 16 TFEU, together with the adoption of a declaration of fundamental rights in the CFREU, enabled the EU to free its regulation from the single market logic. Article 16(1) TFEU confirms that the exercise of the EU’s competence on the protection of personal data and on the free movement of such data is tightly bound to the protection of personal data guaranteed under Article 8 of the CFREU. Such a close relationship is clear if the principles of subsidiarity, necessity, and proportionality are considered: The former suggests that although the EU intervention is justified to “better” regulate the free flow of data among the Member States, it does not empower the EU to protect Union citizens before national

constitutional systems; the latter, instead, imposes on the European Commission the duty to justify its proposals in light of the CFREU – namely Articles 7, 8 and 52(1) – more so than the need to justify the intensity of its action. Therefore, any restriction should be provided by law, the essence of the fundamental right shall be respected, and the limitations placed on the individual's right must fall in line with the general interest recognised by the Union or the need to protect the rights and freedoms of others, and the measure shall be necessary, proportionate and acceptable in any democratic society.

1.3. Article 16 TFEU occupies a cross-cutting position in the founding Treaties, but its horizontality is constrained by the provision of specific rules on PJCCM and by the Member States' prerogative on national security. Moreover, in the AFSJ, the regime on the protection of personal data must respect the different participation of Ireland and Denmark in accordance with Protocols Nos 17, 19, and 20 of the founding Treaties.

By virtue of Article 16(2) TFEU, the EU adopted a new data protection package of “golden rules” that accept restrictions to the individual's right to the protection of personal data in exceptional circumstances. This package is made up of the GDPR, the LED, and the DPREU. The lack of a comprehensive instrument is justified by virtue of Declarations 20 and 21 of the Treaty of Lisbon according to which: on the one hand, specific rules on the protection of personal data and the free movement of such data in the fields of PJCCM could be adopted, if necessary, because of the specific nature of these fields; on the other hand, national security and the regulation of personal data thereto remain fields of competence exclusive to the Member States. On this basis, the LED was adopted to regulate the processing of personal data by those public authorities responsible for the prevention, investigation, detection or prosecution of criminal offences, or for the execution of criminal penalties, including the safeguarding against, and the prevention of, threats to public security, and by any other body or entity entrusted by Member State law to exercise public authority and public powers for these purposes. Compared to the GDPR, the LED significantly restricts, partially or completely, the individuals' rights with respect to the limits established under Article 52(1) of the CFREU.

Last but not least, when applied to the AFSJ, the EU data protection framework must consider that the degrees to which some Member States participate may differ. Specifically, Denmark and Ireland do not fully take part in the AFSJ, yet, some nuances have been highlighted to distinguish those instruments that constitute a development of the Schengen *acquis* from those that are underpinned by the legal bases of the AFSJ alone. While Denmark commits with the Member States and the EU respectively through an international agreement

incorporating those measures it wants to transpose in its national order, Ireland adhered to the PJCCM dispositions stemming from the Convention implementing the Schengen Agreement and benefits from a full opt-in/opt-out regime in the AFSJ.

2. The protection and transfer of personal data according to the EU *acquis*

2.1. In accordance with the *AETR/ERTA* judgment of the CJEU, we concluded that the EU is conferred an (implicit) external competence of a non-exclusive nature.

The GDPR and the LED regulate the transfer of personal data toward a data protection controller or processor, that are subjected or not to the EU *acquis*, as well as to international organisations. We assessed these regimes according to the theory on implied external competences of international organisations to understand their relationship with the existence and nature of the EU external action based on Article 16(2) TFEU. Article 216 TFEU confers on the EU external powers for attaining internal objectives when these objectives are supported by an underlying competence. If *Opinion 1/76* extended this theory to those cases where the EU had not adopted its own legislation, *a fortiori* the *AETR/ERTA* judgment enabled the EU to conclude a treaty once it had adopted its own *acquis*. Having applied the CJEU jurisprudence to the new EU express competence on the protection of personal data and on the free movement of such data, we found that in its external action the EU pursues a specific objective consisting of the prevention of any activity or legislation circumventing the internally established data protection standards. Conversely, Article 16(2) TFEU *per se* does not regulate the transfer or making available of personal data to foreign parties. We maintained that the necessity of the EU intervention is justifiable because of the *effet utile* of its action to attain the objectives pursued under Article 16(2) TFEU.

2.2. The shared nature of the EU's (implied) external competence based on Article 16(2) TFEU modulates the involvement of the EU and its Member States under international law according to the degree of approximation achieved internally: We found that this is more intense in the case of the GDPR and less so in the case of the LED.

Specifically on the nature of the EU's external competence based on Article 16(2) TFEU, we found that the EU has an external non-exclusive competence that covers the domains of the former first/third pillars. The existence of provisions built upon national law, those requiring domestic law to put them into effect, as well as the existence of norms enabling the adoption of provisions more stringent than those the GDPR foresees at national level, or even diverging

from them, led us to the conclusion that the EU is recognised as having an (implied) shared external competence that may be exercised in a mixed manner. The latter solution reflects the Member States' sovereign prerogative, for example, in preserving national security which may be instrumentalised to justify the Member States' participation in the external scene. Conversely, the lower level of harmonisation reached by the LED confers on the EU an (implied) shared competence that responds to the logic of minimum rules. According to the latter, the EU and its Member States are entitled to conclude international agreements that contain the same level of approximation reached by the EU internally, as is the case with the EU-US Umbrella Agreement. This is a LED-based framework agreement setting forth data protection standards to be inserted in future agreements concluded by the EU and the US without impeding the adoption of more stringent rules, though its unenforceability puts into question its validity as a legal basis enabling the transfer of personal data. A forthcoming GDPR-based agreement between the EU and the US was announced by the European Commission on 25 March 2022, but it is due for publication after the end of our research.

2.3. The competence approach allowed us to clarify that adequacy decisions cannot be supplanted by international treaties: The former always constitute a valid legal basis to both protect and transfer personal data, whereas the latter can only be valid legal bases to transfer personal data if they are enforceable in the domestic legal order of the third country or international organisation.

The praetorian doctrine of implied competence inherited by the *AETR/ERTA* case allowed us to better understand the relationship between the so-called adequacy decisions and the EU's treaty-making power underpinned by Article 16(2) TFEU. We assumed that the EU should be recognised to have (implicit) external competence in the personal data field only if an adequacy decision has not been adopted or a "negative" one exists, as is the case with the US following the *Schrems* judgments. From the CJEU's position, it is inferable that the lack of a decision on adequacy cannot be replaced *tout court* by an international agreement that, conversely, requires additional safeguards for the lawful transfer of personal data. If these supplementary measures cannot be adopted, then, data controllers and processors shall suspend or interrupt any transfer toward third parties.

Article 46(2)(a) GDPR, but not Article 37(1)(a) of the LED, emphasises that the agreement through which personal data is transferred must be "enforceable". We have not taken for granted the fact that international agreements meet the "enforceability" requisite and we have maintained that the enforcement of international agreements promoting EU data protection standards in third countries and international organisations shall be read under international

human rights law. The term enforceability is a requirement urging the implementation of data protection safeguards into the municipal legal order of the third country and the international organisation with which the EU concludes an international agreement. In these terms, Convention 108 is enforceable as far as the state at stake is bound by the ECHR too. According to the CJEU's jurisprudence, the actual enforceability of an agreement enabling the transfer of personal data should be assessed by the controller responsible for communicating such data to third parties.

3. The forms and purposes of processing personal data in large-scale IT systems

3.1. AFSJ's large-scale IT systems distinguish from other information networks because they support and participate in the practical implementation of EU policies carried out by national authorities and Union agencies.

Information networks are one of several fields through which the EU implements its policies. In the AFSJ, six large-scale IT systems have been adopted for the implementation of Union policies on borders, visas, police and criminal judicial cooperation, asylum, and migration, namely: the SIS; the VIS; the EES; the ETIAS; the Eurodac, and the ECRIS-TCN. Large-scale IT systems differentiate from other information networks as: they follow a common architecture made of a Central System (C-S) and a National System (N-S); they are provided with a communication infrastructure that has the appropriate capacity to rapidly exchange a considerable volume of data through a secured channel; they store huge volumes and different types of information, including personal data, of many categories of data subjects; they are geographically extended across the entire Schengen area and a variety of authorities can access them; they have been progressively integrated with AI features enabling, for example, mutual automated cross-checking procedures which has in effect converted them into new intelligent technology systems.

3.2. The expansion of the large-scale IT systems' "ancillary purposes" is not only putting into question their lawfulness *vis-à-vis* the principle of purpose limitation, but it is also preventing their systematisation within the AFSJ, as the co-legislators jump from one legal basis to the other without any appearance of planning.

Each large-scale IT system was created to support practical cooperation among Member States and between themselves and the European Commission as a part of a specific Union

policy. Yet, subsequent reforms have been progressively inflated their purposes so much so that the lines separating them have become blurred.

- The SIS was the first system to be implemented following the Convention implementing the Schengen Agreement for PJCCM and border checks purposes so that it could store the personal data of third-country nationals as well as of Union citizens. It was accompanied by the implementation of a communication channel called SIRENE. The SIS has been revised twice: following 11-S as part of the fight against terrorism and in order to allow Europol and Eurojust access to the alerts, provide for the storage of biometrics, and insert specific norms on the protection of personal data; and in 2018 to incorporate the AFIS technology with fingerprints and facial images, to create new categories of alert for irregular migrants, on discreet inquiry, and specific checks, on “Wanted Unknown Persons”, and to increase data protection safeguards.
- The Eurodac was implemented in 2000 to support the Dublin system, as well as the fight against the illegal entry of third-country nationals and – despite recent proposals from the European Commission to further expand its scope, for example, for resettlement and reducing secondary movement by, *inter alia*, storing facial images – it was last revised in 2013 to enable the access of law enforcement authorities and Europol to the data stored therein. The system was accompanied by a communication channel labelled the Dublin Network.
- The VIS Regulation and the VIS LEA Decisions were adopted in 2008 to store the data of short-term visa holders, though access to the system was granted to border guards, immigration authorities, asylum authorities, law enforcement authorities, and Europol as well. In 2021 the VIS Regulation was revised to store the data of long-stay visa owners by virtue of Article 77(2)(a) TFEU, in order to enhance its contribution to the fight against irregular migrants by storing a digital copy of the travel documents, and to lower the age for fingerprinting to six years old. In addition, the new VIS foresees the performance of automated checks against other large-scale IT systems, Europol’s database, and Interpol’s databases SLTD and TDAWN. Despite Article 16 TFEU being proposed as one of the legal bases integrating the legal framework of the revised VIS, it was eventually discarded. The VISION Network enables the consultation among visa authorities and consulates.
- The EES Regulation was adopted in 2017 to record the entry and exit of all third-country nationals authorised to stay within the territories of the Member States for

a short period. It is supposed to become the largest database storing biometric data – namely, fingerprints and facial images – and it serves two main purposes: first, supporting the fight against irregular migration; second, the prevention and combatting of terrorism and serious crimes. In concrete terms, the EES Regulation establishes an “alert bell” that will warn the competent authority when the maximum duration of stay has expired. In addition, both law enforcement authorities and Europol have been granted access to the data stored therein, but their consultation must follow the so-called cascade approach for which they shall consult existing national databases and other decentralised ones – such as the one set forth in the Prüm Decision – and, if a hit occurs, access to the EES shall be prohibited.

- The ETIAS Regulation was adopted in 2018 and it is the sole large-scale IT system that does not contain biometrics, but it holds the largest range of alphanumeric data. The ETIAS is only directed to visa-exempt third-country nationals and aims at strengthening land border checks by calculating who represents a risk to security, irregular migration, or public health. These tasks are not equally important, since ETIAS gravitates more heavily toward security than migration and health objectives, while immigration authorities must consult the EES prior to the ETIAS. For these purposes, ETIAS works through cross-matches with the other large-scale IT systems, the Interpol databases, the ETIAS Watchlist held by Europol and, finally, the so-called screening rules. Only when no hit is detected, the travel authorisation is issued in an automated manner.
- The ECRIS-TCN was agreed in 2019 and it mainly belongs to the criminal judicial cooperation area, though previous convictions can be taken into account for the decisions on ending a legal stay, return, and refusal of entry concerning third-country nationals posing a threat to public policy, public security, or national security. The ECRIS-TCN allows each central authority to find the Member State/s hosting information on a convicted third-country national or dual nationals on a hit/no-hit basis. It might store biometrics – i.e., fingerprints and facial images – and holds alphanumeric data, though biometric identification with facial images has not been agreed for the moment.

3.3. Article 16 TFEU should be envisaged as one of the appropriate legal bases for the legal framework of the AFSJ's large-scale IT systems.

The choice of the correct legal basis underpinning each system is made not according to the centre of gravity theory, but in the light of the purposes for which the data is consulted or accessed. This stance has led to the progressive widening of each large-scale IT system's legal framework, though none have been underpinned by Article 16 TFEU. Following the evolution of the Union's large-scale IT systems, the need to ensure the protection of the processed personal data is becoming widely accepted, as the insertion of enhanced safeguards for the individual testifies. According to CJEU's *Opinion 1/15*, Article 16 TFEU should be pointed out as the appropriate legal basis as the protection of personal data is one of the essential aims or elements of the rules adopted by the EU legislature. Nevertheless, large-scale IT systems are still underpinned only by freedom, security, and justice legal bases. There is reticence in twinning freedom, security, and justice legal bases with Article 16 TFEU, though the principles and rules of the latter clearly play a predominant role.

4. The role played by eu-LISA in the interoperability normative framework

4.1. The blurring of the lines of the freedom, security, and justice goals promoted by the new generations of large-scale IT systems has contributed to the institutionalisation of the operational management of large-scale IT systems within eu-LISA.

The creation of a new Union agency was an indispensable, though questionable, mid-way solution for the integration of the EU "practical" competence on the management of large-scale IT systems, while avoiding any such conferral to the EU. In the lack of an express competence in the founding Treaties, the legal framework of eu-LISA's mandate is made up of substantial Union competences embracing the entire AFSJ, which impacts the participation of Denmark, Ireland, and the Schengen Associated Countries in the agency's governance structure. The legal framework is the same of the IO Regulations, except from Article 16(2) TFEU that is not contemplated and which would have been appropriate in our eyes following the CJEU *Opinion 1/15*.

4.2. eu-LISA's mandate has been progressively broadened without its powers being precisely delineated. There is risk that eu-LISA is delegated the exercise of competences that entail a margin of discretion contrary to the *Meroni* doctrine.

eu-LISA absorbed the European Commission competences on the development, implementation, and operation of the central part of the systems and interoperability components – including the uniform interfaces in the Member States and the related networks – and therefore facilitates the cooperation with and between Member States for the implementation of existing and future large-scale IT systems and interoperability components. Since 2018, eu-LISA has been delegated the elaboration of pilot projects and the management of the communication infrastructure, that it can further delegate to external private entities or bodies. However, the undefined nature and definition of large-scale IT systems and the progressive empowerment of the agency through – e.g., e-CODEX, Prüm, API, and PNR – challenges the principle according to which Union agencies can be delegated ‘precisely delineated powers’.

Although the agency is not delegated decision-making powers, but merely operational ones, our research shows that the agency ends up performing crucial tasks during the design, development, and operational phases of the IT infrastructure of interoperability which might imply a certain degree of discretion. Besides, even if eu-LISA is considered as a “processor” of the data processed therein, we found that it is in fact influencing the ‘purpose and means’ of the processing activities conducted within the large-scale IT systems and interoperability components. Consequently, it would be appropriate to consider that eu-LISA is actually participating in the decision-making process of the competent authorities and Union agencies accessing the data and that its responsibility must be upgraded to the controller level.

4.3. eu-LISA concludes working arrangements both with institutions and agencies of the Union and with third countries and international organisations but, as it does not have access to the data stored in the large-scale IT systems and interoperability components, it cannot communicate them to third parties either.

eu-LISA plays a crucial supportive function with regard to the other freedom, security, and justice agencies of the Union. eu-LISA cooperates with the EBCG Agency in the fields of researching, testing, and developing IT systems, among which the study on biometrics stands out. In the case of the EUAA, eu-LISA has instead adopted a Cooperation Plan to implement

innovative solutions based on the use of AI and machine-learning. It is not clear, however, which guarantees are going to be applied on the processing of (sensitive) personal data.

The transfer of personal data to third countries not subjected to the EU *acquis* and that transferred to international organisations operated by a Union agency is regulated by the EUDPR, whose regime is more fragmentated than those established by the GDPR and the LED, since in no case can Union agencies be delegated political-discretionary powers, but only ‘precisely delineated’ ones according the principle of institutional balance. Articles 46(2)(a) and 46(3)(b) GDPR establish that personal data could be transferred through a legally binding and enforceable instrument or an arrangement, but the latter must ‘include enforceable and effective data subject rights’ and shall be authorised by the competent supervisory authority. According to Article 37(1)(a) and (b) LED, personal data can instead be transferred through a ‘legally binding instrument’ or the controller’s own assessment, which must be communicated to the competent supervisory authority, thus excluding the possibility of concluding soft-law arrangements for transmitting personal data for PJCCM purposes. The EUDPR maintains the GDPR-LED dichotomy, but it also makes safe the cooperation agreement – Article 94(1)(c) EUDPR – and each PJCCM agency’s mandate – Article 94(2) EUDPR – that may maintain or introduce more specific provisions.

eu-LISA is permitted to cooperate with international organisations and other relevant entities by means of working arrangements. These arrangements must be concluded with the authorisation of the Management Board and after having received the approval of the European Commission, without having to consult and receive authorisation from the EDPS. Since eu-LISA has not been granted access to the personal data stored in the large-scale IT systems and interoperability components, our research found that the agency cannot play a direct role in the communication of personal data based on Article 50 of the IO Regulations, but it might with regard to the implementation of the forthcoming agreements, like the EU-Interpol one.

5. The true colors – i.e., circumstances, objectives, and content – of the interoperability framework

5.1. First attempts to establish a framework for interoperability between SIS, Eurodac, and VIS that were made after 11-S did not lead to the adoption of such an instrument for technical, political, and legal reasons.

The first attempts to establish a framework for the interoperability between SIS, Eurodac and VIS were advanced following 11-S but technical, legal, and political concerns prevented

its adoption. The IO Regulations were adopted in 2019 following political agreements concluded in the HLEG chaired by DG HOME with the support of the Council of the EU and the European Parliament. The package was agreed during political trialogues and quickly adopted a few days before the latest parliamentary elections. These circumstances suggest a lack of transparency on the part of the institutions and might have undermined the legislative text in terms of quality, completeness, and attention to human rights. Indeed, soon after their publication in the *OJ*, Regulations (EU) 2019/817 and 2019/818 had to be amended because of the revision to the Visa Code.

5.2. Following the analysis of the IO Regulations, we conclude that they are based on a *sui generis* concept of “correct identification”, which seeks to distinguish individuals – especially third-country nationals – according to a functional logic – i.e., in the absence of a specific competence of the EU – that even goes beyond the objectives of the AFSJ.

The interoperability framework establishes not only an identity management system, but also a case management system. Specifically, the sister Regulations provide for four new objectives:

- first, interoperability gives large-scale IT systems a new IT architecture made of four new components;
- second, interoperability enables the identification of individuals during police checks by virtue of Article 20;
- third, interoperability combats identity fraud and the use of false identities while facilitating the access of *bona fide* travellers in the light of Article 21, and
- fourth, interoperability streamlines the access of law enforcement authorities to the underlying systems under the terms of Article 22.

The purposes of interoperability enshrined in Articles 20, 21, and 22 are considered as new ‘ancillary purposes’ that have been added to the long list of objectives pursued by the underlying large-scale IT systems. This approach gives insight into why interoperability covers the entire sphere of AFSJ without apparently being limited to a specific competence, but rather that it includes: border management, il/legal migration, security, law enforcement and, to a lesser extent, criminal judicial cooperation. In addition, Article 16 TFEU has been inserted as one of the legal bases underpinning this wide legal framework, which is really positive in the light of the CJEU’s *Opinion 1/15*. However, the cross-cutting nature of the interoperability framework does not take into account the differing levels of participation of Member States and Schengen Associated Countries in the Schengen *acquis* and the AFSJ respectively, so that a third regulation would have been needed to respect this dichotomy.

The adoption of a cross-cutting reform aimed at “identifying” individuals’ risks circumventing the limits imposed on the EU by the principle of conferral underpinning each system with a specific legal basis, as was the case with the silo approach. In spite of the Member States’ consensus, the EU has no competence to adopt measures on the identification of third-country nationals *tout court*. However, this may be accepted under the functional rationale if it pursues a specific objective underpinned by a valid legal basis under the founding Treaties. As underlined by the EDPS, the identification of third-country nationals cannot be a purpose on its own, but it should serve a specific objective that must lie within the AFSJ, which is not the case when identification is directed toward unknown persons who are unable to identify themselves or unidentified human remains in case of a natural disaster, accident, or terrorist attack. Such identification instead relies on the Union’s supportive competence on civil protection based on Article 196 TFEU which becomes clear as adherence to Article 20(4) requires a specific action by the Member States. Conversely, when identification supports border checks, police investigations, or legal stays within the EU, then, interoperability exceeds the limits imposed by Article 72 TFEU by assisting national police operations.

Article 21 provides for a multiple-identity detection process following the establishment of coloured links among the identity groups stored in different large-scale IT systems, as long as the links belong to the same person. Thus, interoperability enables the finding of discrepancies between declared identities in different systems, increasing the ability to find identity fraudsters and facilitating the identification of *bona fide* travellers. The multiple-identity detection procedure is made up of two phases that each interfere with the individuals’ rights in different ways. The first automated phase generates white links in case equal or similar identities are detected, or yellow links if the identity of the individual is not clear. According to Article 23 GDPR and Article 11 LED, white links are fully-automated decisions based on sensitive personal data – i.e., biometrics – that must respect different legal limits depending on whether they serve PJCCM purposes or not. If a yellow link is generated, then the second manual verification phase, undertaken by border guards, competent visa authorities, immigration authorities, ETIAS Central Unit and ETIAS National United, SIRENE Bureau, and central authorities of the convicted Member State are called on to resolve the case in question. A white link is established if the authority competent for the manual verification considers that the data belongs to the same person. A green link is established if the authority competent for the manual verification procedure considers that the data belongs to two different persons that have similar identities. A red link indicates a person using different identities in an unjustified manner, or a person using someone else’s identity in an unjustified manner. As for the latter, it is crucial to

recall that red links should lead the authority to neither allege the presence of a public policy or internal security concern, nor use its concerns as justification to issue a SIS alert on refusal of entry. Provided that the links are made up of personal data, the IO Regulations set forth specific guarantees for the individuals to access, erase, and delete their own data. However, as the IO Regulations work on both the GDPR and the LED simultaneously, it is not clear how far the data subjects' rights can be actually restricted. Moreover, from the IO Regulations we inferred that individuals will not receive any informative form when white links are generated in an automated manner, or the authority in charge of the manual verification procedure can establish a green link. Nevertheless, no legislation excludes the possibility that manually established white and green links are erroneous or illegally stored.

Article 22 of the IO Regulations had been proposed with the aim of suppressing the cascade approach by allowing the query of the CIR as far as the EES, the VIS, the ETIAS, and the Eurodac are concerned. Yet, our analysis showed that the cascade approach has not actually been suppressed. According to Article 22, the access of law enforcement authorities and Europol to the data stored in the CIR will be simplified through a two-step approach process: As a first step, the authority, or Europol official, would input the data normally used for accessing the underlying system to retrieve a reference to the system containing the matched data; in the second step, the authority or Europol official would have to access the system/s in case of a match. With the revised VIS Regulation, Article 22 was added to the list of existing requisites to allow law enforcement to access the system, which we find to be positive as it enhances the expectation that the system truly contains data of interest. However, the Proposal for a Prüm II Regulation provides for the implementation of a router enabling the simultaneous query of the Member States' databases, the Europol data, and the CIR via the ESP, and requires the EES, VIS, and ETIAS designated authorities to comply with Article 22. As a result, we alleged that this could be another attempt to circumvent the principle of proportionality by suppressing the cascade approach.

5.3. We highlighted that interoperability's objectives need to be supported by high data quality standards that guarantee reliable outcomes.

These standards depend not only on the provision of specific mechanisms, but also on the circumstances surrounding the insertion of data into the systems and the interoperability components. The IO Regulations foresee that the UMF and the CRRS will also be implemented for semantic and statistical purposes. The elaboration of data for semantic and statistical

purposes not only serves to assist the operational activity of national authorities and Union officials, but also to submit future legislative proposals.

6. Interoperability and the EU's external competence on the protection of personal data and on the free movement of such data

6.1. Given that the ESP is a gateway to a global form of interoperability, it will facilitate the fast, seamless, and quick querying of the EU large-scale IT systems and interoperability components.

The communication of personal data regulated under Article 50 of the IO Regulations should be read in terms of facilitating the identification of third-country nationals whose data is stored in the CIR and, eventually, in the MID. However, the IO Regulations do not clarify which kind of data would be shared in practice.

We analysed Article 50 on the basis of a broad concept of interoperability including both the interconnection of foreign databases with the Union's infrastructure as well as the legibility of the data held by third authorities. As a result of this analysis, we noted that Article 50 was formulated on the basis of three main layers.

- First, Article 50 refers to some of the underlying large-scale IT systems regulations – namely, the VIS, EES, and ETIAS – though we maintained that the SIS, Eurodac, and ECRIS-TCN should also have been foreseen under Regulation (EU) 2019/818.
- Second, Article 50 recalls Articles 25 and 26 of the Europol Regulation, suggesting, in our view, that the EIS could also be interconnected with foreign databases. Although not equipped with their own systems, we alleged that Eurojust, the EBCG Agency, and the EUAA will also contribute to the external dimension of interoperability as far as these agencies conclude international agreements and/or arrangements through which they exchange personal data with third countries and international organisations.
- Third, Article 50 foresees that Interpol's SLTD and TDAWN databases will be interconnected to the CIR via the ESP.

Notably, Article 50 recalls that the act of transferring or making data available should respect the pyramid of tools set forth in Chapter V GDPR, Chapter V LED, and Chapter V EUDPR. We took note of the fact that third countries or international organisations could be subjected to a European Commission adequacy decision, or not. When no adequacy decision is in place, we cautiously highlighted that the transfer data controller must ensure that “appropriate safeguards” are in place and, concretely, that the individual benefits from appropriate redress

mechanisms. Alternatively, we assumed that personal data could be communicated because an administrative agreement or arrangement is in place between a body of the EU, of a third country or of an international organisation. If so, we inspected each agency's mandate in light of the EU data protection *acquis* and the limits established by the delegation doctrine. As a last resort, we considered that the transfer could be based on derogation clauses – i.e., *ad hoc* transfers. Against this background, we assessed the optimal degree of interoperability for each specific situation contemplated under Article 50 according to international and supranational legal standards. As long as interoperability respects these parameters, it is lawful and sustainable – i.e., consistent – *vis-à-vis* the EU internal action. However, the latter precisely might need to be boost with further guarantees that we find necessary to safeguard personal data when this is transferred from/to third parties.

6.2. The communication of personal data to third countries, IOM, UNHCR, and ICRC to return illegally entered/irregular staying migrants, as well as to foreign authorities for PJCCM purposes should be limited to *ad hoc* transfers, based on derogation clauses.

First of all, we noted that the transfer of personal data based on readmission agreements, which are *tout court* considered as “appropriate”, is questionable if it is considered that the clause inserted in these agreements lacks essential data protection elements that would ensure its enforceability. We encourage the co-legislators to strengthen the safeguards provided for in this clause and, more generally, to clarify when we can say that the controller has the necessary tools to ensure that the transfer has “adequate safeguards”. Provided that the transfer of personal data to the IOM, the UNHCR, and the ICRC lacks any adequacy decision or (international) agreement/arrangements, we maintained that interoperability should be kept at the level of *ad hoc* transfers. Although there is no clarity on this point, we maintained that the transfer of data for PJCCM purposes must be relegated to specific derogation clauses instead of appropriate safeguards, which enables the communication of personal data ‘in exceptional cases of urgency’.

6.3. In the absence of an adequacy decision on Interpol, the EU-Interpol Co-operation Agreement would allow for the interoperability of the Union's large-scale IT systems and components with the SLTD and TDAWN databases. However, the negotiation of this Co-operation Agreement must be criticised, as there is strong evidence that not all Interpol's members embrace Union's founding principles – i.e., liberty, democracy and respect for human rights and fundamental freedoms, and the rule of law.

The forthcoming EU-Interpol Cooperation Agreement seeks to: ensure reciprocal direct access to Europol and Interpol databases; interconnect large-scale IT systems – especially the ETIAS – with Interpol's SLTD and TDAWN databases, and grant to Europol, the EBCG Agency, Eurojust, and the EPPO direct access to Interpol's databases. Before concluding such an agreement, the following issues must be taken into account:

- first, the range of the envisaged agreement needs further consideration as long as Interpol's international subjectivity is unclear;
- second, in *WS v Bundesrepublik Deutschland* the CJEU has not ruled on whether this organisation ensures an adequate level of protection to personal data with regard to the EU, and no decision on its level of protection has been adopted so far;
- third, the interconnection of the Interpol's databases with the interoperability infrastructure should in no case reveal red hits to the owner of the alert, as a result, this requires the modification of the Interpol's Rules on Processing of Data, and
- fourth, the Cooperation Agreement risks overflowing into the CFSP where there is no decision regulating the transfer of personal data and lacks consistency with regard to the internal projection of the IO Regulations.

All in all, the envisaged Cooperation Agreement cannot be a statement of principles, but must comply with the requirement of enforceability that ensures effective rights to the individuals affected if it aims at ensuring the systematic consultation of Interpol's databases. If this is not the case, the communication of personal data should be deemed to be regulated by an administrative agreement/arrangement or by derogation clauses.

6.4. The EIS will not migrate into the interoperability infrastructure, instead it will become interoperable with it and could build a bridge with foreign partners' systems on the basis of Europol's international and cooperation agreements. It should be clarified whether Europol's working arrangements respect the prohibition of systematic, massive, or structural transfers as they allow for "sets of transfers".

The EIS stores distinct types of personal data, including sensitive information, belonging to persons suspected of having committed criminal offences, for which Europol is competent, as well as data belonging to victims. It must also be noted that Europol filters the data of people falling outside its mandate, bringing the agency increasingly closer to fulfilling the role of an intelligence service. Although the European Commission's proposal, according to which the agency could have inserted SIS alerts, has finally been rejected, the agency maintains the widest access to large-scale IT systems of any body.

Europol has been tailoring its external activity on the basis of operational agreements through which it could exchange personal data with foreign authorities. The lawfulness of these agreements has been seriously questioned in light of the Council of the EU's close involvement which ultimately bound it. The new Regulation has eliminated the provision on concluding cooperation agreements, but Europol has been granted the possibility to conclude working arrangements, through which it continues exchanging personal data in a contradictory manner: working arrangements are not a valid legal basis for transferring personal data, but they foresee the possibility to transfer it. The Europol Regulation foresees that, in the absence of an adequacy decision, personal data can be transferred through an international agreement concluded by the EU according to Article 218 TFEU. The EDPS recalled that such an agreement should be underpinned by Article 16(2) TFEU and questioned the commitment of some third countries with which negotiations in the human rights field have already started to the EU's position on data protection rights. Although the Europol Regulation states that derogation clauses cannot imply a systematic, massive, or structural transfer, it also confers on the Executive Director the possibility to authorise sets of transfer for one year 'taking into account the existence of adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals'. It is not clear whether these "sets of transfer" always respect the various limits regarding the transfer of personal data or not.

6.5. Unlike Europol, Eurojust has been granted access to two large-scale IT systems out of six: the SIS alerts for police and judicial criminal cooperation and the ECRIS-TCN. Today, the interoperability between the CMS and the Union large-scale IT systems or between the CMS and foreign databases has not been envisaged. Yet, the situation might change in the near future.

The Eurojust's CMS stores various categories of personal data, including sensitive information, in the Index and the TWFs. The regime applicable to Eurojust's processing of personal data varies depending on whether the data is case-related or non-case-related. The former is related to Eurojust's operational activities and concerns criminal investigation or prosecution as well as witnesses or victims; the latter, instead, affects staff members and administrative information.

Eurojust is designated as the point of contact for third countries and international organisations that request the Member States to access the criminal records of a third-country national. If while searching the ECRIS-TCN the agency finds that a Member State holds criminal records for the third-country national in question, it must inform the third party on how to address that Member State if, and only if, that Member State gives its consent. The possibility for Eurojust to receive requests of judicial cooperation turns the agency into a real catalyst as far as international criminal judicial cooperation is concerned.

As with Europol, Eurojust was entrusted with the conclusion of cooperation agreements with third countries and organisations – both international and national – which included the transfer of personal data for operational purposes. Their conclusion outlined a list of countries and international organisations approved by the College of Eurojust and was submitted to the Council for approval. These elements lead us to conclude that they should be considered as executive agreements concluded on behalf of the EU without any real delegation taking place on the basis of the *Meroni* and subsequent rulings. Cooperation agreements have been suppressed with the new Regulation and now the agency can transfer personal data according to: an adequacy decision, an appropriate safeguard, or a specific derogation clause; a cooperation agreement concluded before 12 December 2019, or an international agreement between the EU and the third country or international organisation pursuant to Article 218 TFEU. Consequently, in the case of Eurojust, the exchange of personal data from the EU to third countries and international organisations cannot be channelled through soft law or working arrangements, which is apparently in line with the EUDPR and the Europol Regulation. Yet, the Eurojust Regulation makes safe two relevant instruments: firstly, the Council Common

Position 2005/69/JHA on exchanging personal data with Interpol; and secondly, the Council Decision 2007/533/JHA on the establishment, operation, and use of the SIS II with Interpol.

6.6. The EBCG Agency is the second most important body in the interoperability project given that it has access to four of the six large-scale IT systems, mainly for the purpose of generating statistics, while its ETIAS Central Unit has access to all but one system. The EBCG Agency transfers personal data to third parties via working arrangements or status agreements: the former are soft law instruments that lack democratic backing; the latter have no ‘essential data protection safeguards’.

Provided that the EBCG Agency’s mandate covers both tasks in the field of migration management – most of all on the return of migrants illegally entering the EU – and in the field of serious crime with a cross-border dimension, it is difficult to discern which data protection regime is applicable to the agency’s activities. The EBCG Agency has been increasing its operational tasks exponentially following the humanitarian crisis of 2015 and the same goes for the processing of information. According to the 2019 EBCG Agency Regulation, Member States are obliged to share their information with it and are required to lawfully enter accurate and up-to-date information in European databases. The agency processes personal data in the framework of joint operations, pilot projects, and rapid interventions to return illegal migrants and could combine the data with information on suspicious and/or detected transportation. It also “screens” third-country nationals after disembarkation, and processes personal data concerning persons who the competent authorities of the Member States suspect, on reasonable grounds, of being involved in cross-border criminal activities, in facilitating illegal migration activities, or in human trafficking activities. Moreover, the EBCG Agency’s teams are granted access to large-scale IT systems in the execution of their tasks within the Member States’ territories. Only Regulations (EU) 2018/1861 and 2018/1862 expressly prohibit the interconnection of the SIS ‘[...] to any system for data collection and processing operated by the teams referred to in paragraph 1 or by the European Border and Coast Guard Agency, nor shall the data in SIS to which those teams have access be transferred to such a system’.

The EBCG Agency has been concluding soft working arrangements with third countries and international organisations and these are adopted by the Management Board by absolute majority, after the European Commission’s prior approval and having informed the European Parliament and the Council. Most working arrangements do not specify whether “operational personal data” can be exchanged on their bases, but the 2019 EBCG Agency Regulation allows it in the absence of a status agreement, or if the status agreement does not aim at regulating

personal data processing, or does not contain comprehensive and sufficient data protection safeguards. Status agreements cover all relevant aspects necessary to carry out the agency's tasks, which include provisions on the exchange of information and the transfer of personal data that the EDPS should be aware of. In addition, status agreements provide for a clause on the protection of personal data specifying that while the third country is subject to its national law, the EBCG Agency's teams shall respond to the EUDPR, while Member States' officials respond to the GDPR and the LED. Despite the fact that status agreements offer more guarantees than working arrangements since the former have binding nature, the EDPS warned that the model lacked 'essential data protection safeguards' and should have been developed further in order to comply with EU law.

6.7. It is not clear under which terms the EUAA may be granted access to the large-scale IT systems and the interoperability components, as its Regulation grants the EUAA staff access to both Member States' and European databases. The EUAA may transfer personal data to third countries and international organisations by means of working arrangements that do not guarantee 'enforceable and effective data subjects' rights.

The EUAA's mandate has been recently reformed in order to empower the agency to exchange and analyse information while the Member States must cooperate with its staff. The EUAA can process personal data related to international applications by national administration and authorities, and national and legal developments in the field of asylum, including case law databases. Although the EUAA is not equipped with its own system, it is intended that it develops one in cooperation with eu-LISA. Apart from the elaboration of the Early Warning and Preparedness System based on statistical data, the Asylum Support Teams process personal data while assisting the Member States in the identification and registration of third-country nationals as well as for resettlement purposes.

The EUAA has been mandated to conclude working arrangements with third countries that are ultimately subjected to the European Commission's approval – while the European Parliament and the Council must be informed before their conclusion. These arrangements channel the transfer of personal data to third countries and international organisations (or their bodies) – e.g., to the UNHCR and to the IOM – for the purposes of resettlement: in the absence of a decision on adequacy, or of a legally binding enforceable instrument, these administrative arrangements allow the exchange of personal data with foreign partners at the “operational” level. As with the EBCG Agency, we must be cautious, as the transfer of personal data through soft-law arrangements do not guarantee enforceable and effective rights to the data subject. In

addition, the EUAA Regulation does not contemplate the need of any authorisation from the EDPS in line with Article 48(3)(b) of the EUDPR.

CONCLUSIONES

Empezamos nuestra investigación señalando que, en mayo 2019, la UE aprobó un marco para la interoperabilidad entre los sistemas TI de la UE en materia de fronteras, visados, cooperación policial y judicial criminal, asilo, y migración. Los Reglamentos (UE) 2019/817 y 2019/818 se proponen interconectar los seis sistemas TI de gran magnitud de la UE, ya existentes o de pronta implementación dentro del ELSJ bajo el auspicio de una nueva arquitectura que soportaría su funcionamiento. Estos sistemas son: el SIS; el VIS; el SES; el SEIAV; el Eurodac, y el ECRIS-TCN. La interoperabilidad se define como la habilidad de los sistemas de comunicar, intercambiar datos, y usar la información previamente almacenada en “bases de datos” centralizadas y compartidas. Sin embargo, advertimos que el elevado lenguaje técnico utilizado por el legislador ha llevado a duras críticas que cuestionan su verdadero alcance.

Extendiéndose entre diferentes ordenamientos jurídicos, la interoperabilidad permite a la información y datos personales fluir por varias jurisdicciones, aunque haya diferentes enfoques culturales y jurídicos al derecho a la privacidad, ya que preserva elementos claves de diversidad. Entonces, presentamos la «interoperabilidad legal» como una alternativa a la armonización normativa porque permite la «compatibilidad» de diferentes sistemas jurídicos, sin que la legislación nacional se vea afectada. En concreto, la interoperabilidad entre diferentes jurisdicciones – o interoperabilidad “global” – se basa no en un marco jurídico común en materia de derechos humanos, sino en los principios de reconocimiento mutuo o cooperación para la aplicación: el primero se fundamenta en la presunción de que otros sistemas legales cumplen con los valores comunes que rodean al derecho a la privacidad y el a la protección de los datos personales; el segundo, pretende que el sujeto responsable del tratamiento de datos rinda cuenta por su actividad.

Advertimos que, en el contexto de la UE, la transferencia de datos personales no respaldada por la armonización de los estándares normativos infringe las garantías establecidas en la legislación de la Unión sobre protección de datos personales que, como norma general, requiere que un país tercero o una organización internacional aplique un nivel de protección “equivalente” al de la UE. El derecho humano a la “privacidad”, en sus conceptualizaciones multifacéticas, y el derecho fundamental a la protección de datos personales consagrado por primera vez en el art. 8 de la CDFUE, se ven menoscabados cuando la puesta a disposición de la información del individuo provoca injerencias desproporcionadas. Tras el escándalo Snowden, sistemas jurídicos previamente considerados como “ceranos” al modelo europeo

deben mirarse con sospecha porque han sido juzgados incompatibles con la escala de valores de la UE. Por consiguiente, la “interoperabilidad global” debe ser sopesada con el derecho a la intimidad y el derecho a la protección de los datos personales de forma cuidadosa.

Según el art. 50 de los Reglamentos hermanos, la comunicación de los datos personales a terceros países, organizaciones internacionales y partes privadas se regula por los regímenes sobre protección de datos de los sistemas TI de gran magnitud subyacente y de las agencias de la Unión. Además, los Reglamentos IO avanzan la conclusión de un acuerdo con Interpol que interconectaría la interoperabilidad con las bases de datos SLTD y TDAWN. Los legisladores presentaron el marco jurídico de la interoperabilidad como una solución eficiente y efectiva para alcanzar los objetivos del ELSJ. De hecho, las reglas subyacentes sobre comunicación de datos personales se remiten a las establecidas por la UE en su *acquis* de protección de datos personales, en concreto: el Capítulo V del RGPD; el Capítulo V de la LED, y el Capítulo V del EUDPR. Antes de desarrollar nuestra investigación pre-doctoral, no quedaba claro si y en qué términos la dimensión externa de la interoperabilidad respetaría los parámetros normativos establecidos en el Derecho internacional y en el Derecho de la UE. Por consiguiente, nos hemos preguntado si las normas y los principios aplicables por la UE en caso de comunicación de datos personales a terceras partes son respetado, eludidos o infringidos.

La investigación pre-doctoral ha tenido por objetivo determinar el alcance externo del marco de interoperabilidad establecido por los Reglamentos (UE) 2019/817 y 2019/818, esto es, su extensión más allá de las fronteras exteriores de la UE. Por lo tanto, la tesis ha evaluado si la interoperabilidad de los sistemas centralizados y los componentes de la Unión con bases de datos extranjeras es legal y “sostenible” – i.e., coherente – frente a las normas y principios que fundamentan la acción exterior de la UE. En concreto, hemos pasado en reseña si el art. 50 de los Reglamentos IO cumple con los marcos internacionales y supranacionales y, en su caso, si los derechos de los individuos, sobre todo el derecho fundamental a la protección de los datos personales, son verdaderamente garantizados.

1. El *acquis* de la UE sobre protección de datos personales en el ELSJ

1.1. Ante una respuesta atrasada y suave por parte de la comunidad internacional a la protección del derecho humano a la *privacy* en el nuevo entorno digital, a la UE se le ha atribuido una competencia expresa en materia de protección de datos personales y de libre circulación de estos datos (art. 16 TFUE) desde 2007. Esta base jurídica le otorga un papel de liderazgo mundial en la elaboración y promoción de principios sobre datos personales.

A lo largo del siglo XXI, la revolución tecnológica evidenció que el derecho humano a la privacidad, que había sido consagrado en instrumentos internacionales universales – i.e., el art. 12 de la Declaración Universal de Derechos Humanos (DUDH) y el art. 17 de la Pacto Internacional de Derechos Civiles y Políticos (PIDCP) – debía ser re-interpretado para salvaguardar la dignidad del ser humano en el nuevo entorno digital. Visto que el derecho a la privacidad está extremadamente influenciado por el contexto cultural y jurídico en el que opera, con la Convención 108 del Consejo de Europa consiguió establecer un marco de principios para proteger a los individuos en relación con el procesamiento automático de datos personales. Desde el 1981, la Convención 108 ha representado el mayor punto de referencia para proteger al individuo del uso indebido de las nuevas tecnologías hasta que una competencia específica ha sido atribuida a la UE para adoptar un propio *acquis* sobre protección de datos.

El *acquis* de la UE sobre la protección de datos personales deriva de la integración positiva de supresión de los obstáculos para intercambiar los datos personales entre los Estados miembros derivados de sus legislaciones divergentes. A falta de una competencia expresa atribuida en los Tratados fundacionales, la Comunidad Europea adoptó su propia legislación sobre protección de datos basada en la cláusula de armonización – ahora art. 114 TFEU –, aunque no todos los Estados miembros habían legislado sobre esta materia. La DPD establecía normas mínimas sobre la protección de datos personales y la libre circulación de estos datos, algunas de las cuales son codificadas en la CDFUE. Los principios adicionales sobre la protección de datos personales – como los que se refieren a la seguridad, integridad, y confidencialidad –, en cambio, han sido consolidados por la jurisprudencia del TJUE. El marco intergubernamental que caracteriza las políticas sobre PJCCM legitimó la adopción de un régimen *ad hoc* plasmado en la DPFD, régimen que los Estados miembros han mantenido después de la entrada en vigor del Tratado de Lisboa. En 2007, un artículo nuevo fue insertado en el TFUE y, concretamente, dentro de las disposiciones de aplicación general que atribuyen a la UE una competencia transversal sobre la protección de los datos personales y sobre la libre

circulación de estos datos, con excepción de la Política Exterior y de Seguridad Común (PESC) que se regula por el art. 39 del TUE.

1.2. El art. 16 TFUE atribuye a la UE una competencia compartida en materia de protección de datos personales y de libre circulación de estos datos, cuyo ejercicio responde a los principios de pre-emption, subsidiariedad y proporcionalidad. Por su parte, estos principios deben ser leídos a la luz del derecho fundamental a la protección de los datos personales consagrado en el art. 8 de la CDFUE.

La previsión del art. 16 TFUE, junto a la adopción de una declaración de derechos fundamentales en la CDFUE, permitió a la UE adoptar una regulación desde la lógica del mercado único. El art. 16 TFUE confirma que el ejercicio de la competencia de la UE sobre la protección de datos personales y la libre circulación de estos datos está estrictamente vinculado a la protección de datos garantizada por el art. 8 CDFUE. Esta relación tan estrecha relación se desprende de los principios de subsidiariedad, necesidad, y proporcionalidad: el primero sugiere que aunque la intervención de la UE está justificada para regular “de forma mejor” la libre circulación de los datos entre los Estados miembros, no otorga a la UE el poder para proteger los ciudadanos de la Unión en lugar de los sistemas constitucionales; el segundo, en cambio, obliga a la Comisión Europea a que justifique su propuesta de acuerdo con la CDFUE – o sea, los arts. 7, 8 y 52(1) – más que a la luz de la intensidad de su acción. Por consiguiente: cualquier restricción debe ser establecida por ley, la esencia del derecho fundamental debe ser respetada, las limitaciones deben estar justificadas por objetivos de interés general reconocidos por la Unión o por la necesidad de proteger los derechos y libertades de los demás, y la medida debe ser necesaria y proporcionada en una sociedad democrática.

1.3. El art. 16 TFUE ocupa una posición transversal en los Tratados fundacionales, pero su horizontalidad está coartada por la previsión de normas específicas en materia de PJCCM y por la prerrogativa de los Estados miembros en materia de seguridad nacional. Además, en el ELSJ, el régimen de protección de datos personales debe respetar la diferente participación de Irlanda y Dinamarca de conformidad con los Protocolos 17, 19, y 20 de los Tratados fundacionales.

En virtud del art. 16(2) TFUE, la UE adoptó un nuevo paquete de protección de datos de “reglas de oro” que admiten restricciones a los derechos del individuo en circunstancias excepcionales. Este paquete se compone del RGPD, de la LED, y del EUDPR; la falta de un instrumento comprensivo se justifica a la luz de las Declaraciones 20 y 21 del Tratado de Lisboa por las cuales: por un lado, normas específicas sobre la protección de datos personales y la libre

circulación de estos datos en materia de PJCCM pueden ser adoptadas si es necesario por la especificidad de estos ámbitos; por otro lado, la seguridad nacional y la regulación de datos personales relacionada con ella siguen siendo ámbitos de competencia exclusiva de los Estados miembros. Sobre esta base, la LED fue adoptada para regular el tratamiento de datos personales por las autoridades responsables de la prevención, investigación, detección o enjuiciamiento de las ofensas criminales, o de la ejecución de penas, incluso la salvaguardia contra, y la prevención de, amenazas a la seguridad pública, o por cualquier otro organismo o entidad encargado por la legislación de los Estados miembros de ejercer poderes públicos para estos fines. En comparación con el RGPD, la LED restringe significativamente, de forma parcial o total, los derechos de los individuos con respecto a los límites establecidos en el art. 52(1) de la CDFUE.

Por último, pero no menos importante, cuando el marco de protección de datos de la UE se aplica al ELSJ debe tenerse en cuenta que la participación de algunos Estados miembros puede ser diferente en razón de lo acordado en los Tratados fundacionales. En concreto, Dinamarca e Irlanda no participan plenamente en los instrumentos que constituyen un desarrollo del acervo de Schengen y en los que se apoyan únicamente en las bases jurídicas del ELSJ. Mientras que Dinamarca se compromete con los Estados miembros y con la UE, respectivamente, a través de un acuerdo internacional que incorpora las medidas que desea transponer en su ordenamiento nacional, Irlanda se adhiere a las disposiciones del PJCCM acordadas en el Convenio de aplicación del Acuerdo de Schengen y se beneficia de un régimen completo de *opt-in/opt-out* en el ELSJ.

2. La protección y transferencia de datos personales según el *acquis* de la UE

2.1. De conformidad con la jurisprudencia *AETR/ERTA* del TJUE, hemos concluido que la UE es atribuida una competencia (implícita) externa de naturaleza no exclusiva.

El RGPD y la LED regulan la transferencia de datos personales a un responsable o encargado de protección de datos, independientemente de que esté sujeto al *acquis* de la UE, así como a organizaciones internacionales. Hemos evaluado estos regímenes de conformidad con la teoría sobre las competencias implícitas de las organizaciones internacionales para aclarar su interconexión con la existencia y naturaleza de la acción exterior de la UE basada en el art. 16(2) TFUE. El art. 16(2) TFUE atribuye a la UE el poder para conseguir sus objetivos cuando éstos están previstos en una competencia implícita. Si el *Dictamen 1/16* extendió esta teoría a casos en los que la UE no ha adoptado legislación alguna, *a fortiori* la sentencia *AETR/ERTA*

permitió a la UE concluir un tratado cuando ha desarrollado ya un *acquis* propio. Habiendo aplicado la jurisprudencia del TJUE a la nueva competencia expresa de la UE sobre la protección de datos personales y la libre circulación de estos datos, hemos constatado que en sus relaciones exteriores la UE persigue un objetivo específico que consiste en prevenir que cualquier actividad o disposición eluda los estándares de protección de datos establecidos internamente. Al contrario, el art. 16(2) TFUE *per se* no regula la transferencia de datos o su puesta a disposición a favor de terceras partes extranjeras. Hemos mantenido que la necesidad de intervención de la UE se justifica por el *effet utile* de su acción para alcanzar los objetivos perseguidos por el art. 16(2) del TFUE.

2.2. La naturaleza compartida de la competencia (implícita) exterior de la UE basada en el art. 16(2) TFUE modula la participación de la UE de sus Estados miembros en el Derecho internacional convencional según el grado de aproximación normativa alcanzado internamente: hemos comprobado que este resulta más intenso en el caso del RGPD y menos en el caso de la LED.

En concreto respecto a la naturaleza de la competencia exterior de la UE prevista por el art. 16(2) TFUE, concluimos que la UE tiene una competencia no exclusiva que cubre los ámbitos de los antiguos primer y tercer pilares. La existencia de disposiciones a desarrollarse por ley nacional, es decir, aquellas que requieren que la legislación doméstica las ejecute, así como la existencia de normas que permiten la adopción de reglas más estrictas a nivel nacional que las previstas por el RGPD, nos ha empujado a concluir que la UE es titular de una competencia exterior (implícita) de naturaleza compartida que puede ejercerse de forma mixta. La segunda solución refleja las prerrogativas soberanas de los Estados miembros, por ejemplo, para preservar la seguridad nacional lo que puede ser objeto de instrumentalización por parte de los Estados miembros. Por el contrario, el nivel de aproximación inferior alcanzado por la LED atribuye a la UE una competencia exterior (implícita) que, aun siendo compartida con los Estados miembros, queda atrapada en la lógica de las normas mínimas. Por consiguiente, la UE y sus Estados miembros pueden concluir acuerdos internacionales que contienen el mismo nivel de aproximación alcanzado por la UE internamente, como es el caso del *Umbrella Agreement* entre la UE y los EE.UU. Este acuerdo marco basado en la LED establece estándares en materia de protección de datos que deben ser insertados en acuerdos bilaterales futuros sin impedir la adopción de normas más estrictas, aunque su potencial no ejecución pone en cuestión su validez como base legal para transferir datos personales. Un futuro acuerdo basado en el RGPD entre la UE y EE.UU. fue anunciado por la Comisión Europea el 25 de marzo de 2022, pero aún no se ha publicado al cerrar nuestra investigación.

2.3. El enfoque de competencias nos ha permitido aclarar que las decisiones de adecuación no pueden ser suplantadas por los tratados internacionales: las primeras constituyen siempre una base jurídica válida para proteger y transferir datos personales, mientras que los segundos pueden transferir datos personales solamente si son ejecutables en el ordenamiento jurídico interno del tercer país u organización internacional.

La doctrina pretoriana de las competencias implícitas heredada del caso *AETR/ERTA* nos ha permitido comprender la relación entre las denominadas decisiones de adecuación y la capacidad de la UE para concluir tratados internacionales basada en el art. 16(2) del TFUE. Hemos concluido que la UE debe ser reconocida una competencia externa implícita en materia de protección de datos personales solamente cuando la Comisión Europea no haya adoptado una decisión de adecuación, o existe una decisión “negativa” como en el caso de los EE.UU. tras las sentencias *Schrems*. De la posición adoptada por el TJUE podemos entender que una decisión de adecuación no puede ser reemplazada por un acuerdo internacional *tout court* que, al contrario, requiere garantías adicionales para que la transferencia de datos personales sea legal. En el caso de que medidas de garantía adicionales no puedan ser adoptadas, el responsable y encargado deben suspender o interrumpir cualquier transferencia a terceras partes.

El art. 46(2)(a) del RGPD, pero no el art. 37(1)(a) del LED, subraya que el acuerdo por el cual se transfieren los datos personales debe ser “ejecutable”. No hemos dado por sentado que los acuerdos internacionales cumplan el requisito de ejecución y hemos mantenido que los acuerdos internacionales que promueven las normas de protección de datos de la UE en terceros países y organizaciones internacionales deben leerse con arreglo a la legislación internacional sobre derechos humanos. El término “ejecutable” es un requisito que insta a la aplicación de las garantías de protección de datos en el ordenamiento jurídico municipal del tercer país y de la organización internacional con la que la UE celebra un acuerdo internacional. En estos términos, el Convenio 108 es ejecutable en la medida en que el país en cuestión esté también obligado por el CEDH. Según la jurisprudencia del TJUE, la aplicabilidad real de un acuerdo que permite la transferencia de datos personales debe ser evaluada por el responsable del tratamiento que comunica dichos datos a terceros.

3. Las formas y los objetivos de tratamiento de los datos personales en los sistemas TI de gran magnitud

3.1. Los sistemas IT de gran magnitud del ELSJ se distinguen de otras redes de información porque soportan y participan en la ejecución práctica de las políticas de la UE llevada a cabo por autoridades nacionales y agencias de la Unión.

Las redes de información son una de las distintas formas con las que la UE implementa sus políticas. En el ELSJ, seis sistemas TI de gran magnitud han sido creados para implementar las políticas de la Unión sobre fronteras, visados, cooperación policial y judicial penal, asilo, y migración, en concreto: el SIS; el VIS; el SES; el SEIAV; el Eurodac, y el ECRIS-TCN. Los sistemas TI de gran magnitud se distinguen de otros canales de información porque: siguen un modelo de arquitectura que se compone de un Sistema Central (C-S) y de una Sistema Nacional (N-S); además están provistos de una infraestructura de comunicación que puede intercambiar grandes volúmenes de datos de forma rápida por un canal seguro; almacenan un gran volumen de datos y diferentes tipos de información, también los datos personales, de múltiples categorías de sujetos; se extienden geográficamente en el conjunto del espacio Schengen donde distintas autoridades pueden acceder a ellos. Estos sistemas se han ido conformando progresivamente con elementos de IA que les permiten, por ejemplo, realizar controles recíprocos automatizados, lo cual les convierte en nuevos sistemas de tecnología inteligente.

3.2. La extensión de los “objetivos auxiliares” de los sistemas TI de gran magnitud está no solamente cuestionando su legalidad frente al principio de limitación de la finalidad del primer tratamiento, sino que también impide su sistematización dentro del ELSJ puesto que el legislador salta indistintamente de una base jurídica a la otra.

Cada sistema TI de gran magnitud nació para apoyar la cooperación práctica entre los Estados miembros y entre estos y la Comisión Europea como parte de una política específica de la Unión. Sin embargo, las reformas que se han sucedido progresivamente han inflado sus objetivos hasta difuminar las líneas que les separaban.

- El SIS fue el primer sistema que se puso en marcha tras el Convenio de aplicación del Acuerdo de Schengen a efectos de la PJCCM y de controles fronterizos, de modo que almacena los datos personales de los nacionales de terceros países, así como de los ciudadanos de la Unión. Se le acompañó con la puesta en marcha de un canal de comunicación llamado SIRENE. El SIS ha sido revisado en dos ocasiones: tras el 11-

S en el marco de la lucha contra el terrorismo para permitir a Europol y Eurojust acceder a las descripciones, prever el almacenamiento de datos biométricos e insertar normas específicas sobre la protección de datos personales; y en 2018, para incorporar la tecnología AFIS con huellas dactilares e imágenes faciales, crear nuevas categorías de alerta sobre migración irregular, sobre control discreto, de investigación y específico, y sobre "personas desconocidas buscadas", y aumentar las garantías de protección de datos.

- El Eurodac se puso en marcha en el año 2000 para apoyar el sistema de Dublín, así como la lucha contra la entrada ilegal de nacionales de terceros países, y – a pesar de las recientes propuestas de la Comisión Europea de ampliar su alcance, por ejemplo, para el reasentamiento y la restricción de movimientos secundarios, entre otras cosas, almacenando imágenes faciales – se refundió por última vez en 2013 para permitir el acceso de las autoridades policiales y de Europol a los datos almacenados en él. El sistema estaba respaldado por un canal de comunicación denominado Red de Dublín.
- El Reglamento VIS y las Decisiones VIS LEA se adoptaron en 2008 para almacenar los datos de los titulares de visados de corta duración, aunque también se concedió acceso al sistema a los guardias de fronteras, las autoridades de inmigración, las autoridades de asilo, las autoridades policiales y Europol. En 2021, se revisó el Reglamento del VIS para almacenar los datos de los titulares de visados de larga duración en virtud del art. 77(2)(a) del TFUE, mejorar su contribución a la lucha contra los inmigrantes irregulares almacenando una copia digital de los documentos de viaje, así como para rebajar la edad para tomar las huellas dactilares a seis años. Asimismo, el nuevo VIS prevé la realización de comprobaciones automatizadas con otros sistemas informáticos a gran escala, la base de datos de Europol y las bases de datos SLTD y TDAWN de Interpol. A pesar de que el art. 16 del TFUE se propuso como una de las bases jurídicas que integraban el marco jurídico del VIS revisado, finalmente se descartó. La Red VISION permite la consulta entre las autoridades de visados y los consulados.
- El Reglamento SES se adoptó en 2017 para registrar la entrada y la salida de todos los nacionales de terceros países autorizados a permanecer en el territorio de los Estados miembros durante un breve período. Se supone que se convertirá en la base de datos más amplia que almacena datos biométricos – en concreto, huellas dactilares e imágenes faciales – y sirve para dos fines principales: en primer lugar, la lucha contra la migración irregular; en segundo lugar, la prevención y la lucha contra el

terrorismo y los delitos graves. Concretamente, el Reglamento del SES establece una “alerta” que avisará a la autoridad competente cuando haya expirado la duración máxima de la estancia. Además, tanto las autoridades policiales como Europol tienen acceso a los datos almacenados en él, pero su consulta debe seguir el llamado “enfoque en cascada” según el que, previamente al SES, se consultarán las bases de datos nacionales existentes y otras descentralizadas – como la establecida en la Decisión Prüm – y, en caso de acierto, se prohibirá el acceso al SES.

- El Reglamento SEIAV se adoptó en 2018 y es el único sistema informático de gran magnitud que no contiene datos biométricos, sino la mayor variedad de datos alfanuméricos. El SEIAV está dirigido únicamente a los nacionales de terceros países exentos de visado y tiene como objetivo reforzar los controles en las fronteras terrestres calculando quién representa un riesgo para la seguridad, la migración irregular o de alta epidemia. Estos propósitos no se encuentran en un plano de igualdad, ya que el SEIAV gravita más hacia los objetivos de seguridad que de migración y salud, mientras que las autoridades de inmigración deben consultar el EES antes del SEIAV. Para estos fines, el SEIAV funciona a través de cruces con los otros sistemas informáticos de gran magnitud, las bases de datos de Interpol, la lista de vigilancia del SEIAV en poder de Europol y, por último, las llamadas normas de control. Sólo en caso de que no se detecte ninguna coincidencia, se emite la autorización de viaje de forma automatizada.
- El ECRIS-TCN se acordó en 2019 y pertenece principalmente al ámbito de la cooperación judicial penal, aunque las condenas anteriores pueden tenerse en cuenta para las decisiones de finalización de la estancia legal, devolución y denegación de entrada relativas a nacionales de terceros países que supongan una amenaza para el orden público, la seguridad pública o la seguridad nacional. El ECRIS-TCN permite a toda autoridad central encontrar los Estados miembros en los que se albergan información sobre nacionales de terceros países o personas con doble nacionalidad condenados sobre la base del mecanismo *hit/no-hit*. Podría almacenar datos biométricos – es decir, huellas dactilares e imágenes faciales – y albergar datos alfanuméricos, aunque la identificación biométrica con imágenes faciales no se ha acordado por el momento.

3.3. El art. 16 TFUE debería ser previsto como una de las bases jurídicas adecuadas que integran el marco jurídico de los sistemas TI de gran magnitud del ELSJ.

La elección de la base jurídica adecuada para cada sistema no se realiza en base a la teoría del centro de gravedad, sino a la luz de los objetivos por los cuales los datos son consultados o accedidos. Este enfoque ha ampliado progresivamente el marco jurídico de los sistemas TI a gran magnitud, aunque ninguno ha sido basado en el art. 16 TFUE. Siguiendo la evolución de los sistemas TI de gran magnitud de la Unión, la protección de datos personales ha ganado cada vez más atención como se desprende de la previsión de garantías reforzadas sobre la protección de los datos personales. De conformidad con el *Dictamen 1/15*, el art. 16 debería ser destacado como base jurídica adecuada cuando la protección de datos personales es uno de los objetivos o partes esenciales de las reglas adoptadas en la legislación de la UE. Sin embargo, los sistemas TI de gran magnitud aún se adoptan sobre bases jurídicas del ELSJ solamente. Hay reticencia en doblar bases jurídicas del ELSJ con el art. 16 TFUE, aunque los principios y reglas del segundo juegan un papel evidentemente predominante.

4. El rol de eu-LISA en el marco normativo de interoperabilidad

4.1. Las líneas evanescentes entre los objetivos del ELSJ promovidas por las nuevas generaciones de sistemas TI de gran magnitud contribuyó a la institucionalización de la gestión operativa de estos mismos sistemas en eu-LISA.

La creación de eu-LISA era una solución intermedia indispensable, aunque cuestionable, para el desarrollo de la competencia práctica de la UE para la gestión de los sistemas TI de gran magnitud, evitando la atribución de expresa de competencias a la UE. A falta de una competencia expresa en los Tratados fundacionales, el marco jurídico del mandato de eu-LISA está hecho por competencias sustantivas de la Unión que se refieren a todo el ELSJ, lo cual repercute en la participación de Dinamarca, Irlanda, y los países asociados a Schengen en la estructura gubernativa de la agencia. El marco jurídico es el mismo que los Reglamentos IO, con excepción del art. 16(2) TFUE que no está contemplado a pesar de que habría sido apropiado a nuestro juicio según el *Dictamen 1/15*.

4.2. El mandato de eu-LISA ha sido progresivamente ampliado sin que sus poderes estén precisamente delineados. Existe el riesgo de que a eu-LISA se le deleguen poderes que conlleven un margen de discrecionalidad contrario a la doctrina *Meroni*.

eu-LISA absorbió las competencias de la Comisión Europea sobre el desarrollo, implementación, y operación de la parte central de los sistemas y de los componentes sobre interoperabilidad – incluyendo los interfaces únicos de los Estados miembros y las redes relacionadas – y, por lo tanto, facilita la cooperación con y entre los Estados miembros para la implementación de los sistemas TI de gran magnitud existentes y futuros, así como para los componentes de la interoperabilidad. Desde 2018, a eu-LISA se le delegó la elaboración de proyectos piloto y de la gestión de la infraestructura de comunicación, que puede delegar ulteriormente a entidades y órganos privados externos. Sin embargo, la no definición de la naturaleza de los sistemas TI de gran magnitud y el aumento progresivo del mandato de la agencia – por ejemplo, e-CODEX, Prüm, API, y PNR – contraviene el principio por el cual las agencias de la Unión deben ser objeto de una delegación de ‘poderes precisamente delineados’.

Aunque la agencia carezca de poderes de decisión y haya sido objeto de una delegación de poderes operativos, hemos visto que eu-LISA termina desarrollando tareas cruciales durante las fases de diseño, desarrollo, y operación de la infraestructura TI de la interoperabilidad que puede conllevar un cierto grado de discrecionalidad. Además, y aunque eu-LISA se considera un “encargado” del tratamiento de datos, hemos comprobado que influencia las “finalidades y medidas” de las actividades de tratamiento conducida en los sistemas TI de gran magnitud y en los componentes de la interoperabilidad. Por lo tanto, sería apropiado considerar eu-LISA como participante en el procedimiento de toma de decisiones por parte de las autoridades nacionales y de las agencias de la Unión que acceden a los datos y elevan su estatuto al de responsable del tratamiento.

4.3. eu-LISA concluye acuerdos de trabajo tanto con organismos y agencias de la Unión, como con terceros países y organizaciones internacionales pero, al no tener acceso a los datos personales almacenados en los sistemas TI de gran magnitud y en los componentes de la interoperabilidad, no pudo comunicarlos a terceras partes tampoco.

eu-LISA juega un rol importante de soporte respecto a las agencias de la Unión del ELSJ. eu-LISA coopera con la Agencia EGFC en materias de investigación, pruebas, y desarrollo de los sistemas TI, entre las cuales debemos destacar un estudio sobre datos biométricos. En el caso de la AAUE, en cambio, eu-LISA ha adoptado un Plan de Cooperación para implementar

soluciones novedosas basadas en el uso de la IA y en el aprendizaje automatizado. Pero no está claro que garantías se aplicarán al procesamiento de datos personales (sensibles).

La transferencia de datos personales a terceros países y a organizaciones internacionales gestionadas por una agencia de la Unión está regulada por el EUDPR, cuyo régimen está más fragmentado respecto a los establecidos por el RGPD y la LED, ya que en ningún caso se pueden delegar a las agencias de la Unión poderes político-discrecionales, sino únicamente poderes “exactamente delimitados” según el respeto del principio de equilibrio institucional. Según los arts. 46(2)(a) y 46(3)(b) del RGPD, los datos personales pueden transferirse a través de un instrumento jurídicamente vinculante y ejecutable o de un acuerdo, pero este último debe “incluir derechos exigibles y efectivos del interesado” y debe ser autorizado por la autoridad de control competente. En cambio, según el art. 37(1)(a) y (b) de la LED, los datos personales pueden transferirse mediante un “instrumento jurídicamente vinculante” o la propia evaluación del responsable del tratamiento, que debe ser comunicada a la autoridad de control competente, lo que excluye la posibilidad de celebrar acuerdos de derecho blando para transmitir datos personales a través de ellos con fines de PJCCM. El EUDPR mantiene la dicotomía RGPD-LED, pero también preserva a los acuerdos de cooperación – es decir, el art. 94(1)(c) del EUDPR – y el mandato de cada agencia de PJCCM – es decir, el art. 94(2) del EUDPR, que pueden mantener o introducir disposiciones más específicas.

eu-LISA coopera con organizaciones internacionales y otras entidades relevantes por medio de acuerdos de trabajo. Estos acuerdos deben concluirse con la autorización de su Consejo de Administración y tras haber recibido la aprobación de la Comisión Europea, sin tener que consultar y recibir autorización del SEPD. Visto que eu-LISA no tiene acceso a los datos personales en los sistemas TI de gran magnitud y en los componentes de la interoperabilidad, hemos concluido que la agencia no puede tener ningún rol directo en la comunicación de datos personales basada en el art. 50 de los Reglamentos IO, pero podría tener algún papel respecto a la implementación de futuros acuerdos, por ejemplo, entre la UE e Interpol.

5. La verdadera naturaleza – i.e., circunstancias, objetivos, y contenido – del marco de interoperabilidad

5.1. Las primeras tentativas para establecer un marco para la interoperabilidad entre SIS, Eurodac, y VIS, que se llevaron a cabo después del 11-S, no desembocaron en la adopción de un instrumento por razones técnicas, políticas, y jurídicas.

Las primeras tentativas de establecer un marco para la interoperabilidad entre el SIS, Eurodac y el VIS se adelantaron tras el 11-S, pero problemas técnicos, jurídicos y políticos impidieron su adopción. Los Reglamentos IO fueron adoptados en el 2019 después de los acuerdos políticos del GEAN (Grupo de Expertos de Alto Nivel) moderado por DG HOME con el apoyo del Consejo de la UE y el Parlamento Europeo. El paquete legislativo fue acordado durante los trilogos políticos y fue adoptado rápidamente pocos días después de las últimas elecciones parlamentarias. Estas circunstancias sugieren una falta de transparencia por parte de las instituciones y podrían haber socavado el texto legislativo en términos de calidad, integridad y atención a los derechos humanos. De hecho, en cuanto fueron publicados en el *DO*, los Reglamentos (UE) 2019/817 y 2019/818 fueron emendados en el marco de la revisión del Código de Visados.

5.2. Siguiendo el análisis hecho sobre los Reglamentos IO, concluimos que estos giran alrededor de un concepto de “correcta identificación” *sui generis*, que pretende distinguir a los individuos – sobre todo nacionales de terceros países – bajo una lógica funcional – i.e., a falta de una competencia específica de la UE –, y que incluso extralimita los objetivos del ELSJ.

El marco de interoperabilidad establece no solamente un sistema de gestión de identidades, sino también un sistema de gestión de casos. De forma más concreta, hemos concluido que los Reglamentos hermanos establecen cuatro nuevos objetivos:

- primero, la interoperabilidad confiere a los sistemas TI de gran magnitud una nueva arquitectura hecha por cuatro componentes;
- segundo, la interoperabilidad permite la identificación de los individuos durante los controles policiales ejecutados en virtud del art. 20;
- tercero, la interoperabilidad combate el fraude de identidad y el uso de identidades falsas y garantiza el acceso de los viajeros *bona fide* de acuerdo con el art. 21, y
- cuarto, la interoperabilidad agiliza el acceso de las autoridades de policía a los sistemas subyacentes en los términos del art. 22.

Los objetivos de la interoperabilidad de los arts. 20, 21 y 22 deben considerarse “nuevos objetivos auxiliares” que se añaden al ya larguísimo listado de objetivos perseguidos por los sistemas TI de gran magnitud. Este enfoque da una idea de por qué la interoperabilidad excede el ELSJ, sin aparentemente estar adscrito a una competencia concreta: gestión de frontera, migración regular e irregular, cooperación de policía y, en menor medida, cooperación judicial penal. Es más, el art. 16 TFUE ha sido insertado como una de las bases jurídicas reguladoras de este gran marco jurídico, lo que es realmente positivo a la luz del *Dictamen 1/15* del TJUE. Sin embargo, la naturaleza transversal del marco sobre interoperabilidad no toma nota de la distinta participación de los Estados miembros y de los países asociados a Schengen en el *acquis* homónimo y en el ELSJ, en virtud de cuya dicotomía habría sido necesario adoptar un tercer reglamento.

La adopción de una reforma transversal que persigue “identificar” a los individuos termina eludiendo los límites impuestos a la UE por el principio de atribución que justifica la adopción de cada sistema sobre una base jurídica específica, como se respetaba con el enfoque de silo. A pesar del consentimiento mostrado por los Estados de manera tácita en la práctica, la UE no tiene competencia para adoptar medidas sobre la identificación de migrantes *tout court*, pero esto puede ser aceptado bajo la lógica funcional, si persigue un objetivo específico que se apoye en una base jurídica en los Tratados fundacionales. Como ha sido subrayado por el SEPD, la identificación de nacionales de terceros países no puede ser un objetivo en sí mismo, sino que debe servir un objetivo específico dentro del ELSJ, que no se da cuando la identificación concierne a personas desconocidas que no pueden identificarse o restos humanos no identificados en caso de catástrofe natural, accidente o atentado terrorista. Esta identificación requiere el reconocimiento de una competencia de apoyo de la Unión en materia de protección civil, que se basa en el art. 196 TFUE, como se desprende del hecho de que el art. 20(4) de los Reglamentos IO requiere una acción específica de los Estados miembros. Al contrario, cuando la identificación persigue objetivos en materia de controles de fronteras, cooperación policial, o migración legal, entonces, la interoperabilidad supera los límites impuestos por el artículo 72 del TFUE al ayudar a las operaciones de los policías nacionales.

El art. 21 regula el procedimiento de detección de identidad-múltiple mediante la generación o establecimiento de vínculos por colores entre los grupos de identidad almacenados en los distintos sistemas TI de gran magnitud, siempre y cuando estos pertenecen a una misma persona. En definitiva, la interoperabilidad permite encontrar discrepancias entre las identidades declaradas en los varios sistemas, aumenta la posibilidad de encontrar estafadores de identidades, y facilita la identificación de viajeros *bona fide*. El procedimiento de detección

de identidad-múltiple se compone de dos fases que se interrelacionan de forma diferente con los derechos de los individuos. La primera fase automatizada genera vínculos blancos en caso de que se detecten identidades iguales o similares, o vínculos amarillos si el puzle de identidad no está claro. Según el art. 23 RGPD y el art. 11 LED, los vínculos blancos son decisiones totalmente automatizadas que se basan en datos sensibles – i.e., los datos biométricos – que deben respetar distintos límites impuestos por si sirven objetivos de PJCCM o no. En caso de vínculo amarillo, una segunda fase de verificación manual impone a las guardias de fronteras, a las autoridades competentes para visados, a las autoridades de migración, a la Unidad Central y la Nacional del SEIAV, a la oficina SIRENE, o a las autoridades centrales de los Estados miembros en los que se ha condenado a la persona, resolver el caso al que se enfrenten. Debe establecerse, entonces, un vínculo blanco si la autoridad competente de la verificación manual considera que los datos pertenecen a la misma persona. Un vínculo verde se establece cuando la autoridad competente para el procedimiento de verificación manual considera que los datos pertenecen a dos personas con identidades que comparten algunos puntos en común. Un vínculo rojo se determina que la persona usa diversas identidades de forma injustificada o que la identidad de otra persona de forma injustificada. En este último caso, es importante recordar que el vínculo rojo no debe llevar a la autoridad a alegar la presencia de un problema de orden público o de seguridad interior, ni a asimilar su efecto a una descripción del SIS sobre la denegación de entrada. Visto que los vínculos son datos personales, los Reglamentos IO prevén unas garantías específicas que garantizan el derecho de acceso, rectificación, y supresión de los datos. Aun así, los Reglamentos IO se poyan sobre el RGPD y la LED cumulativamente, y no ha quedado establecido hasta qué punto el sujeto titular de los datos puede verse restringidos esos derechos. Además, de los Reglamentos IO entendemos que los individuos no recibirán el módulo estandarizado cuando los vínculos blancos se general de forma automatizada, o cuando la autoridad encargada de la verificación manual establece un vínculo verde, a pesar de que no se excluye que estos sean erróneos o ilegales.

El art. 22 de los Reglamentos IO fue propuesto con el fin de suprimir el enfoque en cascada y consultar el RCDI respecto a los datos del SES, VIS, SEIAV, y Eurodac, pero esto no ha sido finalmente aceptado. De conformidad con este artículo, el acceso de las autoridades de policía de los Estados miembros y Europol a los datos del RCDI se simplifica en dos pasajes: en el primero, la autoridad o el oficial de Europol insertaría el dato como habitualmente hace para acceder al sistema subyacente para extraer una referencia que contenga el sistema interesado; en el segundo, la autoridad u oficial de Europol deberían tener acceso al sistema, o sistemas, en caso de *match*. Con el Reglamento VIS revisitado, el art. 22 fue añadido al listado de los

requisitos ya existentes para acceder al sistema por parte de las autoridades de policía, lo cual es positivo porque fortalece las expectativas de que ese sistema almacene realmente los datos de interés. Por el contrario, la Propuesta para un Reglamento Prüm II establece la implementación de un *router* que permitirá demandar simultáneamente las bases de datos de los Estados miembros, los datos de Europol, y el RCDI vía el PEB, y requiere a las autoridades designadas del SES, VIS, y SEIAV cumplir tan solo con el art. 22 de los Reglamentos IO. De ahí que advirtiéramos que podría tratarse de un nuevo intento de eludir el principio de proporcionalidad suprimiendo el planteamiento en cascada.

5.3. Destacamos que los objetivos de la interoperabilidad deben estar respaldados por normas de alta calidad de los datos que garanticen resultados fiables.

Estos estándares no sólo dependen de la provisión de mecanismos específicos, sino también de las circunstancias que rodean la inserción de datos en los sistemas y componentes de interoperabilidad. El Reglamento IO prevé que el formato universal de mensajes (UMF) y el repositorio central para la presentación de informes y estadísticas (RCIE) se apliquen también con fines semánticos y estadísticos. La elaboración de datos con fines semánticos y estadísticos no sólo sirve para ayudar a la actividad operativa de las autoridades nacionales y los funcionarios de la Unión, sino también para presentar futuras propuestas legislativas.

6. La interoperabilidad y la competencia exterior de la UE sobre la protección de los datos personales y la libre circulación de estos datos

6.1. La interoperabilidad facilitará la interrogación rápida, sin intermediarios, y directa de los sistemas TI de gran magnitud y de los componentes de la interoperabilidad siendo el PEB una pasarela hacia una forma global de interoperabilidad.

La comunicación de datos personales regulada en el art. 50 de los Reglamentos IO tiene por objetivo agilizar la identificación de los nacionales de terceros países cuyos datos son almacenados en el RCDI y, eventualmente, en el DIM. Sin embargo, los Reglamentos IO no dejan claro qué tipos de datos serán compartidos efectivamente.

Hemos analizado el art. 50 sobre la base de un concepto amplio de interoperabilidad que incluyese tanto la interconexión de bases de datos extranjeras con la infraestructura de la Unión como la legibilidad de los datos por parte de autoridades terceras. Después, hemos visto que el art. 50 se construye sobre tres niveles.

- Primero, el art. 50 se refiere a algunos de los sistemas TI de gran magnitud subyacentes – en concreto, VIS, SES, y SEIAV – pero hemos alegado que SIS, Eurodac, y ECRIS-TCN habrían debido ser previstos también bajo el Reglamento (UE) 2019/818.
- Segundo, el art. 50 se remite a los arts. 25 y 26 del Reglamento de Europol lo cual sugiere que, en nuestra perspectiva, el Sistema de Información de Europol (SIE) podría ser interconectado con bases de datos extranjeras. Aunque no equipadas por sus propios sistemas, hemos avanzado la hipótesis por la cual Eurojust, la Agencia EGFC, y la AAUE contribuyen a la dimensión exterior de la interoperabilidad en la medida en que estas agencias concluyen acuerdos administrativos de derecho duro y/o blando con países terceros y organizaciones internacionales.
- Tercero, el art. 50 establece que las bases de datos SLTD and TDAWN de Interpol serán interconectadas con el RCDI por el PEB.

En particular, el art. 50 recuerda que la transferencia o puesta a disposición de los datos debe respetar la pirámide de herramientas establecida en el Capítulo V del RGPD, el Capítulo V de la LED y el Capítulo V del RPDUE. Tomamos nota del hecho de que terceros países u organizaciones internacionales pueden estar sujetos a una decisión de adecuación de la Comisión Europea, o no. Cuando no existe una decisión de adecuación, advertimos de que el responsable del tratamiento de los datos de la transferencia debe garantizar que existen las “garantías adecuadas” y, concretamente, que la persona se beneficia de los mecanismos de reparación apropiados. Por otra parte, suponíamos que los datos personales podían comunicarse porque existía un acuerdo o convenio administrativo entre un organismo de la UE y un tercer país o una organización internacional. De ser así, hemos examinado el mandato de cada organismo a la luz del acervo de protección de datos de la UE y de los límites establecidos por la doctrina de la delegación. Como último recurso, consideramos que la transferencia podía basarse en cláusulas de excepción – es decir, transferencias *ad hoc*. Sobre la base de este marco, hemos valorado el grado de interoperabilidad óptima para cada una de las situaciones contempladas por el art. 50 de acuerdo con el marco jurídico internacional y supranacional. Mientras la interoperabilidad respete estos parámetros, es lícita y “sostenible” – i.e., coherente – con respecto a la acción interna de la UE. Sin embargo, esto último precisamente podría necesitar ser potenciado con garantías adicionales que consideremos necesarias para salvaguardar los datos personales cuando éstos sean transferidos desde/hacia terceros.

6.2. La comunicación de datos personales a terceros países, la Organización Internacional para las Migraciones (OIM), el Alto Comisionado de Naciones Unidas para los Refugiados (ACNUR), y el Comité Internacional de la Cruz Roja (CICR), para el retorno de migrantes ilegales/irregulares, así como la comunicación de datos personales para finalidades de PJCCM debe ceñirse a transferencias *ad hoc*, basadas en cláusulas de derogación.

En primer lugar, hemos notado que la transferencia de datos basada en los acuerdos de readmisión que se considera “apropiada” sin más inspección, es cuestionable si consideramos que la cláusula prevista en estos acuerdos carece de los elementos esenciales sobre protección de datos que asegurarían su ejecución. Auspiciamos que los legisladores refuercen las garantías previstas en dicha cláusula y que, de forma más genérica, diluciden cuándo podemos afirmar que el responsable del tratamiento dispone de las herramientas necesarias para garantizar que la transferencia disponga de “garantías adecuadas”. Visto que la transferencia de datos personales a la OIM, al ACNUR, y a la CICR no se regula por una decisión de adecuación o un tratado/acuerdo administrativo, hemos concluido que la interoperabilidad debería ser mantenida a nivel de transferencias *ad hoc* de los datos. A pesar de que haya incertidumbre sobre este punto, la comunicación de datos para finalidades de PJCCM se relega a cláusulas de derogaciones específicas, y no a las garantías adecuadas, que permiten la comunicación de datos personales «en casos excepcionales de urgencia» por lo que una interconexión directa debe ser descartada.

6.3. A falta de una decisión de adecuación sobre Interpol, el Acuerdo de Cooperación UE-Interpol permitiría la interoperabilidad de los sistemas TI de gran magnitud y de los componentes de la Unión con las bases de datos SLTD y TDAWN. Sin embargo, la negociación de este Acuerdo de Cooperación debe ser criticada, pues, existen evidencias marcadas de que no todos los países miembros de Interpol comparten los principios fundacionales de la Unión – i.e., libertad, democracia y respeto de los derechos humanos y de las libertades fundamentales y del Estado de Derecho.

El próximo Acuerdo de Cooperación UE-Interpol quiere: garantizar el acceso directo recíproco a las bases de datos respectivas de Europol e Interpol; interconectar los sistemas informáticos de gran magnitud – especialmente el ETIAS – con la base de datos SLTD y TDAWN de Interpol, así como conceder a Europol, a la Agencia EGFC, a Eurojust y a la Fiscalía europea (OPPE) acceso directo a las bases de datos de Interpol. Antes de celebrar dicho acuerdo, deben tenerse en cuenta las siguientes cuestiones:

- en primer lugar, hay que seguir estudiando el alcance del acuerdo previsto mientras tanto no esté clara la subjetividad internacional de Interpol;
- en segundo lugar, en el asunto *WS c Bundesrepublik Deutschland*, el TJUE no se ha pronunciado sobre si esta organización garantiza un nivel adecuado de protección de los datos personales con respecto a la UE, y hasta ahora no se ha adoptado ninguna decisión sobre su nivel de protección;
- en tercer lugar, la interconexión de las bases de datos de Interpol con la infraestructura de interoperabilidad no debería en ningún caso revelar notificaciones rojas al titular de la alerta, lo que requiere la modificación del Reglamento de Interpol sobre el tratamiento de datos, y
- en cuarto lugar, el acuerdo de cooperación corre el riesgo de desbordar la PESC, donde no existe ninguna decisión que regule la transferencia de datos personales, y de carecer de coherencia con respecto a su proyección interna.

En cualquier caso, el Acuerdo de Cooperación previsto no puede ser una declaración de principios, sino que deberá cumplir con el requisito de “ejecutividad” que garantice derechos y garantías efectivos a los individuos afectados si pretende asegurar la consulta sistemática de las bases de datos de Interpol. En caso contrario, la comunicación de datos personales debería considerarse regulada por un acuerdo administrativo o por unas cláusulas de excepción.

6.4. El SIE no migrará a la infraestructura de interoperabilidad, pero será interoperable con la misma y podrá establecer un puente con los sistemas de terceras partes también sobre la base de los acuerdos internacionales o administrativos concluidos por Europol. Se debe aclarar si los acuerdos de trabajo respetan la prohibición de transferencia sistemática, masiva o estructural puesto que permiten “conjuntos de transferencias”.

El SIE almacena distintos tipos de datos personales, también sensibles, que pertenecen a las personas sospechosas de haber cometido un delito criminal, por el cual Europol es competente, así como a las víctimas. Además, Europol filtra los datos de las personas que caen fuera de su mandato, lo cual acerca la agencia cada vez más a los servicios de inteligencia. Aunque la propuesta de la Comisión Europea por la cual la agencia habría podido insertar alertas SIS ha sido rechazada, la agencia tiene garantizado el acceso a todos los sistemas TI de gran magnitud.

Europol ha ido adaptando su actividad exterior sobre la base de acuerdos operativos a través de los cuales podía intercambiar datos personales con autoridades extranjeras. La legalidad de estos acuerdos ha sido seriamente cuestionada a la luz de la estrecha implicación del Consejo de la UE que, en última instancia, vinculaba a éste y no a la agencia. El nuevo Reglamento ha

eliminado la disposición sobre la celebración de acuerdos de cooperación, pero se ha concedido a Europol la posibilidad de celebrar acuerdos de trabajo con los que sigue intercambiando datos personales de forma contradictoria: los acuerdos de trabajo no son una base jurídica válida para transferir datos personales, pero prevén dicha posibilidad. El Reglamento de Europol prevé que, en ausencia de una decisión de adecuación, los datos personales pueden transferirse mediante un acuerdo internacional celebrado por la UE con arreglo al art. 218 del TFUE. El SEPD recordó que dicho acuerdo debería estar respaldado por el art. 16(2) del TFUE y cuestionó el compromiso de algunos terceros países con los que ya se habían iniciado negociaciones por no respetar los derechos humanos. Aunque el Reglamento de Europol establece que estas cláusulas de excepción no pueden implicar una transferencia sistemática, masiva o estructural, también confiere su Director Ejecutivo la posibilidad de autorizar conjuntos de transferencias que no excedan de un año «teniendo en cuenta la existencia de garantías adecuadas con respecto a la protección de la intimidad y de los derechos y libertades fundamentales de las personas». No está claro si los “conjuntos de transferencias” respetan siempre los límites sobre transferencia de datos personales o no.

6.5. A diferencia que Europol, Eurojust tiene acceso a dos de los seis sistemas TI de gran magnitud: las alertas SIS para la cooperación policial y judicial en materia penal y el ECRIS-TCN. En la actualidad, no se ha previsto la interoperabilidad entre el Sistema de Gestión de Casos (SGC) y los sistemas TI de gran magnitud de la Unión o entre el SGC y las bases de datos extranjeras. Sin embargo, la situación podría cambiar en un futuro próximo.

El SGC de Eurojust almacena varias categorías de datos personales, incluidos los sensibles, en el Índice y en los Archivos temporales de Trabajo (ATT) respectivamente. El régimen aplicable al tratamiento de datos personales por parte de Eurojust varía según se trate de datos relacionados o no con casos concretos. Los primeros están relacionados con las actividades operativas de Eurojust y se refieren a la investigación o el enjuiciamiento penal, así como a los testigos o las víctimas; los segundos, en cambio, afectan a los miembros del personal y a la información administrativa.

Eurojust está designado como punto de contacto para los terceros países y las organizaciones internacionales que solicitan a los Estados miembros el acceso a los antecedentes penales de un nacional de un tercer país. Si al buscar en el ECRIS-TCN la agencia descubre que un Estado miembro tiene antecedentes penales del nacional de un tercer país en cuestión, debe informar al tercero sobre cómo dirigirse a ese Estado miembro si, y sólo si, ese Estado miembro da su consentimiento. La posibilidad de que Eurojust reciba solicitudes de cooperación judicial

convierte a la agencia en un verdadero catalizador en lo que respecta a la cooperación judicial penal internacional.

Al igual que Europol, Eurojust recibió el mandato de celebrar acuerdos de cooperación con terceros países y organizaciones – tanto internacionales como nacionales – que incluían la transferencia de datos personales con fines operativos. Su celebración seguía una lista de países y organizaciones internacionales aprobada por el Colegio de Eurojust y se presentaba al Consejo para su aprobación. Estos elementos nos llevan a concluir que deben considerarse como acuerdos ejecutivos celebrados en nombre de la UE sin que se produzca una verdadera delegación sobre la base de la sentencia *Meroni* y posteriores. Los acuerdos de cooperación se han suprimido con el nuevo Reglamento y ahora la agencia puede transferir datos personales con arreglo a: una decisión de adecuación, o una salvaguardia adecuada, o una cláusula de excepción específica; un acuerdo de cooperación celebrado antes del 12 de diciembre de 2019, o un acuerdo internacional entre la UE y el tercer país u organización internacional con arreglo al art. 218 del TFUE. Por consiguiente, en el caso de Eurojust, el intercambio de datos personales de la UE con terceros países y organizaciones internacionales no puede canalizarse a través de normas no vinculantes o acuerdos de trabajo, lo que aparentemente está en consonancia con el EUDPR y el Reglamento de Europol. Sin embargo, el Reglamento Eurojust pone a salvo dos instrumentos relevantes: en primer lugar, la Posición Común 2005/69/JAI del Consejo sobre el intercambio de datos personales con Interpol; y en segundo lugar, la Decisión 2007/533/JAI del Consejo relativa al establecimiento, funcionamiento y utilización del SIS II con Interpol.

6.6. La Agencia EGFC es el segundo órgano más importante para el proyecto de interoperabilidad si se considera que tiene acceso a cuatro de los seis sistemas TI de gran magnitud, sobre todo para finalidades estadísticas, mientras que a la Unidad Central del SEIAV le falta solo uno. La Agencia EGFC transfiere datos personales a terceras partes vía acuerdos de trabajo o acuerdos de estatuto: los primeros son acuerdos de derecho blando que carecen de respaldo democrático; los segundos no prevén «salvaguardias esenciales para la protección de datos».

Visto que el mandato de la Agencia EGFC cubre tanto tareas en materia de gestión de migraciones – sobre todo para el retorno de los migrantes que entran ilegalmente al territorio de la Unión – y en materia de delitos graves con una dimensión transfronteriza, es difícil entender qué régimen de protección de datos personales se aplica a sus actividades. La Agencia EGFC ha ido aumentando sus tareas operativas de forma exponencial tras la crisis humanitaria de 2015 y lo mismo ocurre con el tratamiento de la información. Según el Reglamento de la

Agencia EGFC de 2019, los Estados miembros están obligados a compartir su información con ella y a introducir legalmente información precisa y actualizada en las bases de datos europeas. La agencia procesa datos personales en el marco de operaciones conjuntas, proyectos piloto e intervenciones rápidas de retorno de inmigrantes ilegales y podría combinar los datos con información sobre transportes sospechosos y/o detectados. También “controla” a los nacionales de terceros países tras su desembarco, y trata los datos personales de las personas de las que las autoridades competentes de los Estados miembros sospechan, por motivos razonables, que estén implicadas en actividades delictivas transfronterizas, en la facilitación de actividades de migración ilegal o en actividades de trata de seres humanos. Es más, los equipos de la Agencia EGFC tienen garantizado el acceso a los sistemas de información de gran magnitud en la ejecución de sus tareas en el territorio de los Estados miembros. Solo los Reglamentos (UE) 2018/1861 y 2018/1862 prohíben expresamente la interconexión del SIS «[...] a cualquier sistema de recogida y tratamiento de datos gestionado por los equipos mencionados en el apartado 1 o por la Agencia Europea de la Guardia de Fronteras y Costas, ni se transferirán a dicho sistema los datos del SIS a los que tengan acceso dichos equipos».

La Agencia EGFC ha venido celebrando acuerdos de trabajo blandos con terceros países y organizaciones internacionales, que son adoptados por el Consejo de Administración por mayoría absoluta, previa aprobación de la Comisión Europea y tras haber informado al Parlamento Europeo y al Consejo. La mayoría de los acuerdos de trabajo no especifica si los “datos personales operativos” pueden intercambiarse bajo los auspicios de dichos acuerdos blandos, pero el Reglamento de la Agencia EGFC de 2019 los considera como una base jurídica válida en ausencia de un acuerdo de estatuto, o en caso de que el acuerdo de estatuto no tenga como objetivo regular el tratamiento de datos personales o no contenga garantías de protección de datos completas y suficientes. Los acuerdos de estatuto cubren todos los aspectos pertinentes necesarios para llevar a cabo la acción de la agencia, entre los que se incluyen las disposiciones sobre el intercambio de información y la transferencia de datos personales que el SEPD debe conocer. Asimismo, los acuerdos de estatuto prevén una cláusula sobre la protección de los datos personales que especifica que, mientras el tercer país está sujeto a su legislación nacional, los equipos de la Agencia EGFC responderán al RGPD, mientras que los funcionarios de los Estados miembros responderán al RGPD y al LED. No obstante, el SEPD afirmó que el modelo carecía de «salvaguardias esenciales para la protección de datos» y que debería haberse desarrollado más para cumplir con la legislación de la UE.

6.7. No está claro en qué términos se puede conceder a la AAUE el acceso a los sistemas TI de gran magnitud y a los componentes de interoperabilidad, ya que su Reglamento concede al personal acceso tanto a las bases de datos de los Estados miembros como a las europeas. La AAUE puede transferir datos personales a terceros países y organizaciones internacionales por medio de acuerdos de trabajo que no garantizan «derechos ejecutables y efectivos de los interesados».

El mandato de la AAUE se ha reformado recientemente para facultar a la agencia a intercambiar y analizar información, mientras que los Estados miembros deben cooperar con su personal. La AAUE puede procesar datos personales relacionados con las solicitudes de protección internacional por parte de la administración y las autoridades nacionales, así como la evolución nacional y jurídica en el ámbito del asilo, incluidas las bases de datos de jurisprudencia. Aunque la AAUE no está dotada de un sistema propio, se supone que desarrollará uno en cooperación con eu-LISA. Aparte de la elaboración del Sistema de Alerta Temprana y Preparación basado en datos estadísticos, los Equipos de Apoyo al Asilo procesan datos personales al tiempo que asisten a los Estados miembros en la identificación y registro de nacionales de terceros países, así como a efectos de reasentamiento.

La AAUE ha recibido el mandato de celebrar acuerdos de trabajo con terceros países que, en última instancia, están sujetos a la aprobación de la Comisión Europea, mientras que el Parlamento Europeo y el Consejo son informados antes de su celebración. Estos acuerdos canalizan la transferencia de datos personales a terceros países y organizaciones internacionales – por ejemplo, al ACNUR y a la OIM – con fines de reasentamiento: a falta de una decisión de adecuación, o de un instrumento jurídicamente vinculante, estos acuerdos administrativos permiten el intercambio de datos personales con socios extranjeros a nivel “operativo”. Como es el caso de la Agencia EGFC, debemos advertir que la transferencia de datos personales a través de acuerdos de derecho blando no garantiza “derechos ejecutables y efectivos de los interesados”. Además, el Reglamento de la AAUE no contempla la necesidad de ninguna autorización por parte del SEPD, en consonancia con el artículo 48(3)(b) del EUDPR.

CONCLUSIONI

La nostra ricerca è iniziata segnalando che, nel maggio 2019, l'UE ha adottato un quadro di riferimento per l'interoperabilità tra i sistemi IT dell'UE relativi agli ambiti delle frontiere, dei visti, della cooperazione di polizia e giudiziaria penale, dell'asilo e della migrazione. I Regolamenti (UE) 2019/817 e 2019/818 mirano ad ottenere l'interconnessione dei sei sistemi IT su larga scala dell'Unione, già esistenti o di prossima realizzazione all'interno dello SLSG, con il proposito di implementare una nuova architettura informatica che supporterà il loro funzionamento. Si tratta dei sistemi SIS, VIS, EES, ETIAS, Eurodac e ECRIS-TCN. Per interoperabilità s'intende la capacità dei sistemi di comunicare, scambiare dati e utilizzare le informazioni precedentemente archiviate in database centralizzati e condivisi. Eppure, abbiamo notato che i complessi tecnicismi utilizzati dal legislatore hanno portato a dure critiche da parte di coloro che diffidano della vera portata di questa riforma.

Estendendosi tra vari sistemi giuridici, l'interoperabilità consente al flusso di informazioni e dati personali di scorrere tra molteplici giurisdizioni anche qualora i sistemi di tutela della *privacy* divergano per ragioni culturali e giuridiche, mantenendo quegli elementi chiave che causano discrepanze. Ciò detto, abbiamo introdotto la "interoperabilità giuridica" come un'alternativa all'armonizzazione normativa poiché permette la "compatibilità" di sistemi giuridici divergenti senza richiedere l'armonizzazione delle legislazioni sottostanti. Segnatamente, l'interoperabilità tra giurisdizioni differenti (o interoperabilità "globale") si fonda non su un quadro giuridico comune in materia di diritti umani, ma sui principi del mutuo riconoscimento e della cooperazione eseguita all'interno di ciascun ordinamento: da una parte vi è la presunzione che altri sistemi giuridici rispettino valori comuni, quali la tutela della *privacy* e dei dati personali; dall'altra il soggetto responsabile del trattamento deve dimostrare di adempiere alle norme e principi concordati.

Abbiamo messo in luce come, all'interno dell'Unione, il trasferimento dei dati personali in assenza di standard normativi armonizzati fa venir meno le garanzie stabilite dalla legislazione dell'Unione in materia di dati personali, che di norma richiede al Paese terzo o all'organizzazione internazionale di adottare un livello di protezione "equivalente" al proprio. Nella sua natura pluridimensionale, il diritto umano alla "*privacy*" e il diritto alla tutela dei dati personali, sancito per la prima volta dall'art. 8 della CDFUE, possono essere violati nei casi in cui la divulgazione delle informazioni relative all'interessato costituisca un'intromissione sproporzionata. In seguito allo scandalo Snowden, anche sistemi giuridici ritenuti in passato "vicini" al modello europeo devono essere guardati con sospetto, poiché si sono rivelati

incompatibili con la gerarchia di valori dell'UE. Pertanto, la “interoperabilità globale” e i diritti dell'individuo alla *privacy* e alla protezione dei dati personali devono essere bilanciati con attenzione.

Secondo l'art. 50 dei Regolamenti fratelli, la comunicazione dei dati personali a Paesi terzi, organizzazioni internazionali e privati è disciplinata dalle regole stabilite per i sistemi IT su larga scala sottostanti e dai regimi imposti alle agenzie dell'Unione per il trasferimento dei dati personali. I Regolamenti IO introducono inoltre un nuovo accordo con Interpol, che collegherebbe l'interoperabilità alle banche dati SLTD e TDAWN. I co-legislatori hanno presentato il quadro giuridico dell'interoperabilità come una soluzione efficace ed efficiente per la gestione degli obiettivi dello SLSG. Di fatti, le norme soggiacenti alla comunicazione dei dati personali rimandano a quelle disposizioni definite dall'UE nella propria normativa sulla protezione dei dati personali, ovvero: il Capo V del RGPD, il Capo V della LED, ed il Capo V del EUDPR. Prima di intraprendere la nostra ricerca, non si sapeva se e in quali termini la dimensione esterna dell'interoperabilità rispettasse i parametri normativi stabiliti nel diritto internazionale e nel diritto dell'UE. Abbiamo quindi analizzato se le norme e i principi applicati dall'UE in caso di comunicazione dei dati personali a terzi fossero stati rispettati, elusi, o violati dal quadro giuridico dell'interoperabilità.

Lo studio condotto a livello di dottorato di ricerca si è concentrato sulla definizione della portata esterna del quadro dell'interoperabilità stabilito dai Regolamenti (UE) 2019/817 e 2019/818, ovvero sulla loro estensione oltre i confini esterni dell'UE. Questa tesi ha dunque considerato se l'interoperabilità tra i sistemi e le componenti centralizzate dell'Unione e i database esteri fosse legittima, nonché “sostenibile” (ovvero coerente), rispetto alle norme e ai principi che regolano l'azione esterna dell'UE. Segnatamente, si è analizzata la conformità dell'art. 50 dei Regolamenti IO rispetto ai parametri giuridici internazionali e sovranazionali e, quando positivamente accertata, abbiamo esaminato l'effettiva garanzia dei diritti dell'individuo, con particolare riferimento al diritto alla protezione dei dati personali.

1. L'*acquis* dell'UE sulla protezione dei dati personali nello SLSG

1.1. A fronte di una risposta tardiva e poco incisiva da parte della comunità internazionale per tutelare del diritto umano alla *privacy* nel nuovo contesto digitale, nel 2007 all'UE è stata conferita una competenza esplicita in materia di protezione dei dati personali e di libera circolazione di tali dati (art. 16 del TFUE), che le ha garantito il ruolo di *leadership* nell'elaborazione e nella promozione globale di nuovi principi per la salvaguardia dei dati personali.

La rivoluzione tecnologica del secolo XXI ha messo in luce l'esigenza di una nuova interpretazione del diritto umano alla *privacy*, già consacrato in strumenti internazionali universali, quali l'art. 12 della Dichiarazione Universale dei Diritti Umani (DUDU) e l'art. 7 della Convenzione Internazionale sui Diritti Civili e Politici (CIDCP), al fine di tutelare la dignità della persona all'interno del nuovo contesto digitale. Tale diritto è chiaramente influenzato dalle circostanze culturali e giuridiche in cui si applica tanto che, relativamente al trattamento automatico dei dati personali, la Convenzione 108 del Consiglio d'Europa ha potuto stabilire un quadro di riferimento che sancisce solo principi generali. Fin dal 1981, la Convenzione 108 ha rappresentato il punto di riferimento per la tutela dell'individuo contro l'uso improprio delle nuove tecnologie, fino a quando all'UE è stata conferita una competenza specifica, sulla cui base ha adottato un proprio regime sulla protezione dei dati personali. L'*acquis* dell'Unione sulla protezione dei dati personali deriva dalla logica dell'integrazione positiva volta a rimuovere gli ostacoli imposti allo scambio dei dati personali tra gli Stati membri a causa dell'esistenza di legislazioni divergenti. In assenza di una competenza espressamente conferita dai Trattati istitutivi, la Comunità europea aveva già adottato una propria legislazione sulla protezione dei dati personali giustificata sulla base della clausola di armonizzazione (attuale art. 114 TFUE), ma non tutti gli Stati membri avevano legiferato in questa materia. La DPD ha stabilito norme minime sulla protezione dei dati personali e sulla libera circolazione di tali dati, alcune codificate nella CDFUE. La giurisprudenza della CGUE, poi, ha integrato ulteriori principi per proteggere i dati personali, tra cui quelli della sicurezza, integrità e riservatezza. Il quadro intergovernativo delle politiche in materia di PJCCM, invece, ha portato all'adozione di un regime *ad hoc*, stabilito nella DPF, che gli Stati membri hanno mantenuto anche dopo l'entrata in vigore del Trattato di Lisbona. Nel 2007, il TFUE è stato provvisto di un nuovo articolo tra le disposizioni di applicazione generale che riconosce all'UE una competenza orizzontale sulla tutela dei dati personali e sulla libera circolazione di tali dati, con un'unica eccezione: l'art. 39 TUE in materia di Politica Estera e di Sicurezza Comune (PESC).

1.2. L'art. 16 del TFUE conferisce all'UE una competenza concorrente in materia di protezione dei dati personali e di libera circolazione di tali dati, il cui esercizio risponde ai principi di pre-emption, di sussidiarietà e di proporzionalità. A loro volta, questi principi devono essere letti alla luce del diritto fondamentale alla protezione dei dati personali sancito nell'art. 8 della CDFUE.

Le disposizioni dell'art. 16 TFUE, unitamente all'adozione di una dichiarazione dei diritti fondamentali nella CDFUE, hanno consentito all'UE di svincolare la regolamentazione pre-Lisbona dalla logica del mercato unico. L'art. 16(1) TFUE conferma che l'esercizio della competenza dell'UE sulla protezione dei dati personali e sulla libera circolazione di tali dati è strettamente correlata alla protezione dei dati personali garantita dall'art. 8 CDFUE. Tale nesso risulta evidente se si analizzano i principi di sussidiarietà, necessità e proporzionalità. Il primo sancisce che sebbene l'intervento dell'UE sia giustificato nell'ottica di una “migliore” regolamentazione per liberare il flusso di dati personali tra gli Stati membri, questo non conferisce priorità all'Unione sulla tutela dei diritti fondamentali dei cittadini rispetto ai sistemi costituzionali nazionali; il secondo impone alla Commissione europea di giustificare le proprie proposte legislative alla luce della CDFUE, ovvero dei suoi arts. 7, 8 e 52(1), piuttosto che alla luce dell'intensità dell'azione dell'Unione. In particolare rilevano: il principio di legalità, per cui ogni restrizione deve essere imposta per legge; la salvaguardia dell'essenza dei diritti fondamentali in questione, che deve essere sempre e comunque preservata; la giustificazione dei limiti ad ogni restrizione che deve perseguire obiettivi di interesse generale riconosciuti dall'Unione, o la necessità di tutelare i diritti e le libertà altrui, e la necessità e proporzionalità di suddette misure rispetto a criteri accettabili in qualsiasi società democratica.

1.3. L'art. 16 del TFUE occupa una posizione trasversale nei Trattati istitutivi, ma la sua orizzontalità è limitata dalla presenza di norme specifiche sulla PJCCM e dalla prerogativa degli Stati membri in materia di sicurezza nazionale. Inoltre, nello SLSG, il regime di protezione dei dati personali deve rispettare la diversa partecipazione dell'Irlanda e della Danimarca, conformemente ai Protocolli 17, 19 e 20 dei Trattati istitutivi.

Ai sensi dell'art. 16(2) TFUE, l'UE ha adottato un nuovo pacchetto di “regole d'oro” sulla protezione dei dati che ammette restrizioni ai diritti dell'individuo solamente in circostanze eccezionali. Tale pacchetto include il GDPR, la LED e il EUDPR. L'assenza di uno strumento olistico è giustificata dalle Dichiarazioni 20 e 21 del Trattato di Lisbona, che stabiliscono la possibilità di adottare norme specifiche per la protezione dei dati personali e per la libera circolazione di tali dati negli ambiti del PJCCM qualora la natura specifica di tali ambiti lo

richieda. Inoltre, esse confermano la competenza esclusiva degli Stati membri in materia di sicurezza nazionale e sulla regolamentazione dei dati personali correlati. La LED è stata adottata proprio in questo contesto, al fine di regolamentare il trattamento dei dati personali da parte delle autorità competenti sulla prevenzione, indagine, accertamento e persecuzione di reati o esecuzione di sanzioni penali, così come da parte di qualsiasi altro ente o entità incaricata dalla legge di uno Stato membro di esercitare la pubblica autorità e i poteri pubblici diretti a tali scopi. A confronto con il RGPD, nella LED i diritti degli individui risultano significativamente circoscritti, parzialmente o totalmente, se si prendono in considerazione i limiti definiti dall'art. 52(1) della CDFUE.

Infine, l'applicazione del quadro dell'UE sulla protezione dei dati personali nello SLSG deve prendere in considerazione possibili variazioni di partecipazione da parte di alcuni Stati membri. In particolare, la Danimarca e l'Irlanda non partecipano a tutto lo SLSG. Occorre distinguere, infatti, quegli strumenti che rappresentano uno sviluppo dell'*acquis* Schengen, da quelli che si fondano esclusivamente sulle basi giuridiche dello SLSG. La Danimarca si vincola nei confronti degli Stati membri e dell'UE con la ratifica di un accordo internazionale che prevede misure da trasporre al proprio ordinamento; l'Irlanda, invece, ha aderito alle disposizioni della PJCCM concordate nella Convenzione di Applicazione dell'Accordo di Schengen e gode interamente del diritto di non partecipare allo SLSG.

2. La protezione ed il trasferimento dei dati personali secondo l'*acquis* dell'UE

2.1. Alla luce della giurisprudenza *AETR/ERTA* della CGUE, abbiamo concluso che all'UE è attribuita una competenza esterna (implicita) di natura non esclusiva.

Il RGPD e la LED disciplinano il trasferimento dei dati personali verso un titolare o responsabile del trattamento, soggetti o no all'*acquis* dell'UE, oltre che verso organizzazioni internazionali. Al fine di definire il rapporto tra l'esistenza e la natura dell'azione esterna dell'Unione in base all'art. 16(2) TFUE, abbiamo esaminato le norme sul trasferimento dei dati personali secondo la teoria delle competenze esterne implicite delle organizzazioni internazionali. L'art. 216 TFUE conferisce all'UE poteri esterni volti a perseguire obiettivi interni, qualora tali obiettivi siano supportati da una competenza soggiacente. Se il *Parere 1/76* ha ampliato questa teoria ai casi in cui l'UE non ha adottato una legislazione propria, *a fortiori* la sentenza *AERT/ERTA* ha consentito all'UE di concludere un accordo internazionale dopo essersi dotata di un proprio *acquis*. Applicata la giurisprudenza della CGUE alla nuova competenza esplicita dell'Unione sulla protezione dei dati personali e sulla libera circolazione di tali dati, abbiamo riscontrato come l'azione esterna dell'UE sia volta alla persecuzione di un

obiettivo specifico, ovvero la prevenzione di qualsiasi attività o legislazione che eluda gli standard di protezione dei dati applicati internamente. Al contrario, l'art. 16(2) TFEU non disciplina di per sé il trasferimento o la messa a disposizione dei dati personali a parti terze. Abbiamo sostenuto che la necessità d'intervento dell'UE è giustificabile in virtù dell'*effet utile* che le azioni della stessa apportano al raggiungimento degli obiettivi di cui all'art. 16(2) TFEU.

2.2. La natura concorrente della competenza esterna (implicita) dell'UE, basata sull'art. 16(2) del TFUE, modula il coinvolgimento dell'UE e dei suoi Stati membri alla luce del diritto internazionale in base al grado di ravvicinamento normativo raggiunto internamente: abbiamo riscontrato che questo è più intenso nel caso del GDPR, e meno nel caso della LED.

Con particolare riferimento alla natura della competenza esterna dell'UE basata sull'art. 16(2) TFUE, abbiamo concluso che l'UE gode di una competenza esterna non esclusiva che copre gli ambiti dei precedenti primo e terzo pilastri. L'esistenza di disposizioni fondate sul diritto nazionale, che richiedono all'ordinamento corrispondente di eseguirle, così come di norme che prevedono l'adozione di disposizioni più severe rispetto a quelle previste dal RGPD a livello nazionale, o che se ne distanziano persino, ci hanno spinto a concludere che la competenza dell'UE ha natura esterna concorrente (implicita) e può essere esercitata in modalità mista. Quest'ultima soluzione riflette la prerogativa sovrana degli Stati membri, per esempio, in materia di sicurezza nazionale che può divenire uno strumento utile per giustificare la partecipazione degli stessi nello scenario estero. Al contrario, il livello inferiore di armonizzazione raggiunto dalla LED riconosce all'UE una competenza concorrente (implicita) vincolata dalla logica delle norme minime. UE e Stati membri, quindi, hanno il potere di concludere trattati internazionali che prevedono lo stesso livello di approssimazione raggiunto dall'UE internamente, come nel caso dell'*Umbrella Agreement* tra UE e US. Quest'ultimo costituisce un accordo il cui ambito di applicazione coincide con la LED e definisce gli standard per la protezione dei dati personali che integreranno accordi futuri, senza impedire agli Stati membri l'adozione di norme più severe. Tuttavia, la natura non esecutiva dell'*Agreement* esclude la sua validità come base giuridica in grado di consentire il trasferimento dei dati personali. Il 25 marzo 2022, la Commissione europea ha preannunciato la negoziazione di un nuovo accordo basato sul RGPD tra l'UE e gli US che non abbiamo potuto esaminare perché non era stato ancora pubblicato quando abbiamo chiuso la nostra ricerca.

2.3. L’approccio sulle competenze ci ha permesso di chiarire perché le decisioni di adeguatezza non possono essere sostituite dai trattati internazionali: le prime costituiscono sempre una base giuridica valida per proteggere e trasferire dati personali; i secondi possono essere validi per il trasferimento di dati personali solo se sono resi esecutivi nell’ordinamento giuridico interno del Paese terzo o organizzazione internazionale.

La dottrina pretoriana sulle competenze implicite sviluppata a partire dal caso *AETR/ERTA* ha consentito una migliore comprensione della relazione tra le cosiddette decisioni di adeguatezza e il potere di concludere trattati dell’UE, basato sull’art. 16(2) TFUE. Siamo partiti dall’ipotesi per cui attribuiamo all’UE una competenza esterna implicita nell’ambito dei dati personali solo in assenza di una decisione di adeguatezza o in presenza di una tale decisione “negativa”, come nel caso degli US dopo la saga *Schrems*. La posizione della CGUE lascia inferire che l’assenza di una decisione di adeguatezza non può essere semplicemente sostituita da un accordo internazionale che, invece, prevede ulteriori tutele per il trasferimento legittimo dei dati personali. Qualora non sia possibile adottare tali misure supplementari, i titolari e i responsabili dei dati dovranno sospendere o interrompere qualsiasi trasferimento verso terzi.

L’art. 46(2) GDPR, ma non l’art. 37(1) LED, pone l’accento sul fatto che l’accordo alla base del trasferimento dei dati personali deve essere “esecutivo”. Non abbiamo dato per scontato che gli accordi internazionali soddisfino il requisito della “esecutività” e abbiamo sostenuto che l’applicazione degli accordi internazionali che promuovono gli standard di protezione dei dati dell’UE di fronte a Paesi terzi e organizzazioni internazionali deve essere letta alla luce del diritto internazionale dei diritti umani. Il termine “esecutivo” è un requisito che richiede l’attuazione di tutele di protezione dei dati a livello degli ordinamenti giuridici locali del Paese terzo e dell’organizzazione internazionale con cui l’UE conclude l’accordo internazionale. In tal senso, la Convenzione 108 è esecutiva nella misura in cui lo Paese in questione è a sua volta vincolato dalla CEDU. In base alla giurisprudenza della CGUE, l’effettiva natura esecutiva di un accordo che consente il trasferimento di dati personali deve essere valutata dal titolare e dal responsabile della comunicazione dei dati a terzi.

3. Le forme e gli obiettivi del trattamento dei dati personali nei sistemi IT su larga scala dello SLSG

3.1. I sistemi IT su larga scala dello SLSG si distinguono da altre reti di comunicazione perché sostengono e partecipano all’attuazione pratica delle politiche dell’UE da parte delle autorità nazionali e delle agenzie dell’UE.

Le reti di comunicazione sono uno dei diversi modi con cui l’UE attua le proprie politiche. Nello SLSG sono stati adottati sei sistemi IT su larga scala per l’implementazione delle politiche dell’Unione su frontiere, visti, cooperazione di polizia e giudiziaria penale, asilo, e migrazioni, ovvero: il SIS; il VIS; l’EES; l’ETIAS; l’Eurodac, e l’ECRIS-TCN. I sistemi IT su larga scala si differenziano da altre forme di reti di comunicazione perché: seguono un’architettura comune composta da un sistema centrale (C-S) e un sistema nazionale (N-S); sono dotati di un’infrastruttura di comunicazione che ha la capacità di scambiare rapidamente un volume considerevole di dati attraverso un canale sicuro; conservano enormi volumi e diversi tipi di informazioni, compresi i dati personali, di molte persone; si estendono geograficamente a tutta l’area Schengen nella quale differenti categorie di autorità possono accedervi; sono stati progressivamente integrati con elementi di AI che permettono, per esempio, di eseguire controlli incrociati di dati automatizzati, il che li converte in nuovi sistemi a tecnologia intelligente.

3.2. L’estensione degli “obiettivi ancillari” dei sistemi IT su larga scala non solo pone in dubbio la loro legalità di fronte al principio della finalità del primo trattamento, ma impedisce anche la loro sistematizzazione nello SLSG poiché il legislatore si muove indistintamente da una base giuridica all’altra.

Ciascun sistema IT su larga scala è nato per supportare la cooperazione pratica tra gli Stati membri, e tra questi e la Commissione europea, come parte di una competenza specifica dell’Unione. Tuttavia, le riforme successive dei sistemi IT su larga scala hanno progressivamente gonfiato i loro obiettivi sino a sfumare le linee che dividevano ciascun’area di appartenenza.

- Il SIS è stato il primo sistema ad essere adottato in seguito alla Convenzione di applicazione dell’Accordo di Schengen ai fini della PJCCM e dei controlli alle frontiere, in modo da memorizzare i dati personali dei cittadini di Paesi terzi e dei cittadini dell’Unione. È stato accompagnato dalla realizzazione di un canale di

comunicazione chiamato SIRENE. Il SIS è stato riformato due volte: dopo l'11-S a all'insegna della lotta al terrorismo per consentire a Europol e Eurojust di accedere alle segnalazioni, prevedere la memorizzazione di dati biometrici, e inserire norme specifiche sulla protezione dei dati personali; e nel 2018 per incorporare la tecnologia AFIS con impronte digitali e immagini facciali, creare nuove categorie di segnalazione sull'immigrazione irregolare, sul controllo discreto, di indagine e specifico e sui "ricercati ignoti", così come per aumentare le garanzie in materia di protezione dei dati.

- L'Eurodac è stato implementato nel 2000 per sostenere il sistema di Dublino e la lotta contro l'ingresso illegale di cittadini di Paesi terzi e, nonostante le recenti proposte della Commissione europea di ampliare ulteriormente il suo campo di applicazione, ad esempio, per il reinsediamento e contro i movimenti secondari, tra le altre cose, memorizzando immagini facciali, è stato da ultimo rifiuto nel 2013 per consentire l'accesso delle autorità di polizia e di Europol ai dati in esso memorizzati. Il sistema è affiancato da un canale di comunicazione denominato *Dublin Network*.
- Il Regolamento VIS e la decisione VIS LEA sono stati adottati nel 2008 per memorizzare i dati dei titolari di visti per soggiorni di breve durata, anche se l'accesso al sistema è stato concesso anche alla polizia di frontiera, alle autorità di immigrazione, alle autorità di asilo, alle autorità di polizia e anche a Europol. Nel 2021 il Regolamento VIS è stato modificato per memorizzare i dati dei titolari di un visto per il soggiorno di lunga durata ex art. 77(2)(a) del TFUE, migliorare il suo contributo alla lotta contro i migranti irregolari memorizzando una copia digitale dei documenti di viaggio, e abbassare l'età per il rilevamento delle impronte digitali a sei anni. Inoltre, il nuovo VIS prevede l'esecuzione di controlli automatizzati con altri sistemi IT su larga scala, il database di Europol e le banche dati SLTD e TDAWN di Interpol. Nonostante l'art. 16 del TFUE sia stato proposto come una delle basi giuridiche che integrano il quadro giuridico del nuovo VIS, quest'ipotesi alla fine è stata scartata. La rete VISION permette alle autorità competenti in materia di visto e ai consolati di consultarsi tra di loro.
- Il Regolamento EES è stato adottato nel 2017 per registrare l'entrata e l'uscita di tutti i cittadini di Paesi terzi autorizzati a soggiornare nel territorio degli Stati membri per un breve periodo. Dovrebbe diventare la più ampia banca dati che conserva dati biometrici – vale a dire, impronte digitali e immagini facciali – e serve a due scopi principali: primo, alla lotta contro l'immigrazione irregolare; secondo, alla

prevenzione e la lotta contro il terrorismo e i reati gravi. Concretamente, il regolamento EES stabilisce un “campanello d’allarme” che avviserà l’autorità competente quando la durata massima del soggiorno è scaduta. Inoltre, sia le autorità di polizia che Europol hanno ottenuto l’accesso ai dati ivi memorizzati, ma la loro consultazione deve seguire il cosiddetto “approccio a cascata” per cui, prima dell’EES, dovranno consultarsi le banche dati nazionali esistenti e le altre banche dati decentralizzate – come quella stabilita nella Decisione Prüm – e, in caso di *hit*, l’accesso al EES è vietato.

- Il Regolamento ETIAS è stato adottato nel 2018 ed è l’unico sistema informatico su larga scala che non contiene dati biometrici, ma la più grande varietà di dati alfanumerici. L’ETIAS è diretto solo ai cittadini di Paesi terzi esenti dal visto e mira a rafforzare i controlli alle frontiere terrestri calcolando chi rappresenta un rischio per la sicurezza, l’immigrazione irregolare o l’epidemia grave. Tuttavia, questi scopi non sono ugualmente importanti poiché l’ETIAS gravita più pesantemente attorno alla sicurezza piuttosto che agli obiettivi di migrazione e salute, tanto che le autorità d’immigrazione devono consultare l’EES prima dell’ETIAS. Per questi scopi, l’ETIAS funziona mediante confronti incrociati con altri sistemi informatici su larga scala, le banche dati di Interpol, la *Watchlist* detenuta da Europol e, infine, le cosiddette regole di *screening*. Solo nel caso in cui non venga rilevato alcun *hit*, allora, l’autorizzazione di viaggio viene rilasciata in modo automatico.
- L’ECRIS-TCN è stato concordato nel 2019 e appartiene principalmente al settore della cooperazione giudiziaria penale, anche se le condanne penali possono essere prese in considerazione per le decisioni sulla fine del soggiorno legale, il rimpatrio e il rifiuto d’ingresso per i cittadini di Paesi terzi che rappresentano una minaccia per l’ordine pubblico, la sicurezza pubblica o la sicurezza nazionale. L’ECRIS-TCN permette ad ogni autorità centrale di trovare lo Stato membro o gli Stati membri che possiedono informazioni sul casellario giudiziario dei cittadini di Paesi terzi o cittadini con doppia nazionalità su una base *hit/no-hit*. Può memorizzare dati biometrici – cioè impronte digitali e immagini facciali – e conserva dati alfanumerici, anche se l’identificazione biometrica per mezzo di immagini facciali non è obbligatoria per il momento.

3.3. L'art. 16 del TFUE dovrebbe essere considerato una delle basi giuridiche appropriate da inserire in ciascun quadro giuridico dei sistemi IT su larga scala dello SLSG.

La scelta della base giuridica che regola ciascun sistema è fatta alla luce delle finalità per cui i dati sono consultati o accessi piuttosto che in ragione della teoria del centro di gravità. Questo approccio ha progressivamente ampliato il quadro giuridico di ogni sistema IT su larga scala, anche se nessuno di questi è stato sostenuto dall'art. 16(2) del TFUE. In seguito all'evoluzione dei sistemi IT su larga scala dell'Unione, la protezione dei dati personali ha guadagnato sempre più l'attenzione dei co-legislatori, come testimonia l'inserimento di garanzie rafforzate per l'individuo in ciascuna regolamentazione riguardante i sistemi. Secondo il *Parere 1/15* della CGUE, l'art. 16 del TFUE dovrebbe essere indicato come base giuridica appropriata quando la protezione dei dati personali è una delle finalità o componenti essenziali delle norme adottate dal legislatore dell'UE. Tuttavia, i sistemi IT su larga scala sono ancora supportati solo da basi giuridiche dello SLSG. C'è reticenza nel gemellare le basi giuridiche dello SLSG con l'art. 16 del TFUE, anche se i principi e le regole di quest'ultimo giocano chiaramente un ruolo predominante.

4. Il ruolo di eu-LISA nel quadro normativo dell'interoperabilità

4.1. L'offuscamento degli obiettivi di libertà, sicurezza e giustizia promosso dalle nuove generazioni di sistemi IT su larga scala ha contribuito all'istituzionalizzazione della gestione operativa degli stessi in eu-LISA.

La creazione di una nuova agenzia dell'Unione è stata un'indispensabile, anche se discutibile, via intermedia per integrare la competenza "pratica" dell'UE sulla gestione dei sistemi IT su larga scala, evitando il conferimento diretto all'Unione. In mancanza di una competenza esplicita nei Trattati istitutivi, il quadro giuridico del mandato di eu-LISA è costituito da competenze sostanziali dell'Unione che abbracciano l'intero SLSG, il che influisce nella partecipazione della Danimarca, l'Irlanda e dei Paesi associati a Schengen nella struttura di *governance* dell'agenzia. Il quadro giuridico è lo stesso dei Regolamenti IO, ad eccezione dell'art. 16(2) del TFUE, che non è stato contemplato nonostante la sua previsione sarebbe stata appropriata alla luce dell'interpretazione fatta dalla CGUE nel *Parere 1/15*.

4.2. Il mandato di eu-LISA è stato progressivamente ampliato senza che le sue competenze siano state delineate con precisione. C'è il rischio che a eu-LISA siano delegati poteri che comportano un margine di discrezionalità contrario alla dottrina *Meroni*.

eu-LISA ha assorbito le competenze della Commissione europea sullo sviluppo, l'implementazione e il funzionamento delle parti centrali dei sistemi e delle componenti dell'interoperabilità – comprese le interfacce uniformi negli Stati membri e le relative reti di comunicazione – e quindi facilita la cooperazione con e tra gli Stati membri grazie all'implementazione dei sistemi IT su larga scala, esistenti e futuri, e delle componenti dell'interoperabilità. Dal 2018, a eu-LISA è stata delegata l'elaborazione di progetti pilota e la gestione dell'infrastruttura di comunicazione, che può ulteriormente delegare a enti o organismi privati esterni. Tuttavia, la natura indefinita dei sistemi IT su larga scala e la progressiva responsabilizzazione dell'agenzia – con, ad esempio, e-CODEX, Prüm, API e PNR – contraddice il principio secondo cui alle agenzie dell'Unione possono essere delegati solo «poteri precisamente delineati».

Anche se a eu-LISA non sono stati delegati poteri decisionali, ma solo operativi, abbiamo rilevato che eu-LISA finisce per avere un ruolo di fondamentale importanza durante le fasi di progettazione, sviluppo e funzionamento dell'infrastruttura IT dell'interoperabilità, il che potrebbe implicare un certo grado di discrezionalità. Inoltre, anche se eu-LISA è considerata come “responsabile” del trattamento dei dati, abbiamo scoperto che la stessa sta realmente influenzando lo “scopo e i mezzi” delle attività di trattamento dei dati condotte all'interno dei sistemi IT su larga scala e dei componenti delle interoperabilità. Di conseguenza, sarebbe opportuno considerare eu-LISA come una parte del processo decisionale insieme alle autorità competenti e le agenzie dell'Unione che accedono ai dati e, quindi, elevare la sua responsabilità al livello di titolare del trattamento.

4.3. eu-LISA conclude intese di lavoro sia con organismi e agenzie dell'Unione che con Paesi terzi e organizzazioni internazionali ma, non avendo accesso ai dati personali conservati nei sistemi IT su larga scala e alle componenti dell'interoperabilità, non può nemmeno comunicarli a terzi.

eu-LISA svolge una funzione di supporto cruciale nei confronti delle altre agenzie dello SLISG dell'Unione. eu-LISA coopera con l'Agenzia EGFC nel campo della ricerca, dei test e dello sviluppo dei sistemi IT, tra cui spicca lo studio della biometria. Nel caso dell'EUAA, invece, eu-LISA ha adottato un piano di cooperazione per implementare soluzioni innovative

basate sull'uso della AI e del *machine-learning*. Non è chiaro, però, quali garanzie verranno applicate al trattamento dei dati personali (sensibili).

Il trasferimento di dati personali a Paesi terzi non soggetti all'*acquis* dell'UE e a organizzazioni internazionali gestite da un'agenzia dell'Unione è regolato dal EUDPR, il cui regime appare più frammentato rispetto a quello stabilito dal RGPD e dalla LED, poiché in nessun caso le agenzie dell'Unione possono essere delegate poteri politico-discrezionali, ma solo quelli “precisamente delineati” nel rispetto del principio di equilibrio istituzionale. Secondo gli artt. 46(2)(a) e 46(3)(b) del RGPD, i dati personali potrebbero essere trasferiti attraverso uno strumento giuridicamente vincolante ed esecutivo o qualsiasi altro tipo di intesa, ma quest'ultima deve «includere diritti esecutivi ed effettivi degli interessati» e deve essere autorizzato dall'autorità di controllo competente. Secondo l'art. 37(1)(a) e (b) LED, invece, i dati personali possono essere trasferiti attraverso «uno strumento giuridicamente vincolante» o una valutazione del responsabile del trattamento che deve essere comunicata all'autorità di controllo competente, escludendo così la possibilità di concludere accordi *soft-law* per la trasmissione di dati personali per scopi di PJCCM. Il EUDPR mantiene la dicotomia GDPR-LED, ma fa salvi anche gli accordi di cooperazione – l'art. 94(1)(c) EUDPR – e il mandato di ciascuna agenzia nell'ambito della PJCCM – cioè l'art. 94(2) EUDPR – che può mantenere o introdurre disposizioni più specifiche.

eu-LISA è autorizzata a cooperare con organizzazioni internazionali e altre entità pertinenti mediante intese di lavoro. Queste intese devono essere concluse con l'autorizzazione del suo Consiglio di Amministrazione e dopo aver ricevuto l'approvazione della Commissione europea, senza dover consultare e ricevere l'autorizzazione del Garante Europeo sulla Protezione Dati (GEPD). Poiché a eu-LISA non è stato concesso l'accesso ai dati personali memorizzati nei sistemi IT su larga scala e nelle componenti dell'interoperabilità, abbiamo riscontrato che l'agenzia non può svolgere un ruolo diretto nella comunicazione dei dati personali in base all'art. 50 dei Regolamenti IO, ma potrebbe essere involucrata in altro modo, ad esempio, nell'attuazione di futuri accordi, come quello previsto tra UE-Interpol.

5. La vera natura – i.e., circostanze, obiettivi, e contenuto – del quadro normativo sull'interoperabilità

5.1. I primi tentativi di stabilire un quadro per l'interoperabilità tra SIS, Eurodac e VIS sono stati perseguiti dopo l'11-S, ma questo non è stato adottato per problemi tecnici, giuridici e politici.

I Regolamenti IO sono stati adottati nel 2019 a seguito di accordi politici conclusi nel *High Level Expert Group* (HLEG) presieduto da DG HOME, con il sostegno del Consiglio dell'UE

e del Parlamento europeo. Il pacchetto è stato concordato durante triloghi politici e poi rapidamente adottato pochi giorni prima delle ultime elezioni parlamentari. Queste circostanze suggeriscono una mancanza di trasparenza da parte delle istituzioni e potrebbero aver compromesso il testo legislativo in termini di qualità, completezza e attenzione verso i diritti umani. Di fatti, subito dopo la loro pubblicazione in *GU*, i Regolamenti (UE) 2019/817 e 2019/818 sono stati modificati a causa della revisione del Codice sui Visti.

5.2. In seguito all’analisi condotta sui Regolamenti IO, abbiamo scoperto che questi istituiscono un concetto *sui generis* di “identificazione corretta” che mira a distinguere gli individui – soprattutto i nazionali di Paesi terzi – secondo una logica funzionale – ossia in assenza di una specifica competenza dell’UE – che va persino al di là degli obiettivi dello SLSG.

In termini generali, abbiamo concluso che il quadro sull’interoperabilità stabilisce non solo un sistema di gestione dell’identità, ma anche un sistema di gestione di casi. In particolare, i Regolamenti fratelli prevedono quattro nuovi obiettivi:

- primo, l’interoperabilità dà ai sistemi IT su larga scala una nuova architettura informatica fatta di quattro nuove componenti;
- secondo, l’interoperabilità permette l’identificazione delle persone durante i controlli di polizia ex art. 20;
- terzo, l’interoperabilità combatte la frode d’identità e l’uso di identità false, facilitando l’accesso dei viaggiatori di buona fede in virtù dell’art. 21, e
- quarto, l’interoperabilità razionalizza l’accesso delle autorità di polizia ai sistemi sottostanti ai sensi dell’art. 22.

Gli scopi dell’interoperabilità sanciti dagli artt. 20, 21 e 22 sono considerati come nuovi “scopi accessori” che sono stati aggiunti alla lunga lista degli obiettivi perseguiti dai sistemi IT su larga scala. Questo approccio dà un’idea del perché l’interoperabilità avvolga l’intero SLSG senza essere apparentemente limitata da una competenza specifica: gestione delle frontiere, migrazione il/legale, sicurezza, cooperazione di polizia e, in misura minore, cooperazione giudiziaria penale. Di conseguenza, l’art. 16 del TFUE è stato inserito – il che è davvero positivo alla luce del *Parere 1/15* della CGUE – come una delle basi giuridiche a sostegno di un quadro giuridico già di per sé molto ampio. Tuttavia, la natura trasversale del quadro dell’interoperabilità non tiene conto della diversa partecipazione degli Stati membri e dei Paesi associati a Schengen nell’*acquis* omonimo e nello SLSG, perché per rispettare questa dicotomia si sarebbe dovuto adottare un terzo regolamento.

L'adozione di una riforma orizzontale volta a "identificare" l'individuo rischia di eludere i limiti imposti all'UE dal principio di attribuzione per cui ogni sistema poggia su una base giuridica specifica, come è stato rispettato con l'approccio a silo. Nonostante il consenso degli Stati membri, l'UE non è competente per adottare misure sull'identificazione di cittadini di Paesi terzi *tout court*, ma ciò può essere accettato secondo la logica funzionale per cui si persegue un obiettivo specifico sostenuto da una base giuridica valida ai sensi dei Trattati istitutivi. Come sottolineato dal GEPD, l'identificazione di nazionali di Paesi terzi non può essere uno scopo a sé stante, ma deve servire un obiettivo specifico calato all'interno dello SLSG; questo non è certo il caso dell'identificazione volta a persone sconosciute che non sono in grado di identificarsi, o volta a resti umani non identificati in caso di disastro naturale, incidente, o attacco terroristico. Tale identificazione risponde alla competenza di sostegno dell'Unione in materia di protezione civile ex art. 196 del TFUE, il che si deduce dal fatto che l'adesione all'art. 20(4) dei Regolamenti IO non è obbligatoria e richiede un'azione specifica da parte degli Stati membri. Quando l'identificazione serve per i controlli di frontiera, alle indagini di polizia o ai soggiorni legali all'interno dell'UE, i limiti imposti dall'art. 72 del TFUE non sono stati comunque rispettati.

L'art. 21 prevede un processo di rilevamento di identità multiple in seguito alla creazione di legami colorati tra i gruppi di identità memorizzati in diversi sistemi IT su larga scala, a condizione che appartengano alla stessa persona. Così, l'interoperabilità permette di trovare discrepanze tra le identità dichiarate in diversi sistemi, aumentando la possibilità di trovare truffatori di identità e facilitando l'identificazione dei viaggiatori di buona fede. La procedura di rilevamento dell'identità multiple è composta da due fasi che interferiscono in modo diverso con i diritti della persona. La prima fase automatizzata genera *links* bianchi nel caso in cui vengano rilevate identità uguali o simili, o *links* gialli se il puzzle dell'identità non è molto chiaro. Secondo l'art. 23 GDPR e l'art. 11 LED, i collegamenti bianchi sono decisioni completamente automatizzate basate su dati personali sensibili – cioè la biometria – che devono rispettare diversi limiti legali a seconda che servano o meno a scopi PJCCM. Nel caso in cui venga generato un collegamento giallo, invece, nella seconda fase di verifica manuale la polizia di frontiera, le autorità competenti in materia di visti, le autorità di immigrazione, l'Unità Centrale ETIAS e l'Unità Nazionale ETIAS, l'ufficio SIRENE e le autorità centrali dello Stato membro del casellario giudiziario sono chiamate a risolvere il caso in questione. Si deve stabilire un legame bianco se l'autorità competente per la verifica manuale ritiene che i dati appartengano alla stessa persona. Un collegamento verde, invece, deve crearsi se l'autorità competente per la procedura di verifica manuale ritiene che i dati appartengano a due persone

diverse che hanno identità condividenti alcuni dati. Un collegamento rosso indica una persona che usa identità diverse in modo ingiustificato o una persona che usa l'identità di qualcun altro in modo ingiustificato. Per quanto riguarda quest'ultimo, è fondamentale ricordare che i collegamenti rossi non devono indurre l'autorità competente a sospettare della presenza di un problema di ordine pubblico o di sicurezza interna, né ad assimilare il suo effetto a una segnalazione SIS di rifiuto d'ingresso. Dato che i *links* sono dati personali, i Regolamenti IO stabiliscono garanzie specifiche per gli individui di accedere, rettificare e cancellare i propri dati. Tuttavia, poiché i Regolamenti IO si basano contemporaneamente sul RGPD e sulla LED, non è chiaro fino a che punto i diritti degli interessati possano essere effettivamente limitati. Inoltre, dai Regolamenti IO abbiamo dedotto che gli individui non riceveranno alcun modulo standard quando i *links* bianchi sono generati in modo automatizzato, o l'autorità incaricata della procedura di verifica manuale stabilisce un *link* verde. Tuttavia, nulla esclude che sia i *links* bianchi che quelli verdi siano errati o memorizzati illegalmente.

L'art. 22 del Regolamento IO era stato proposto con l'obiettivo di sopprimere l'approccio a cascata, consentendo l'interrogazione dell'EES, il VIS, l'ETIAS e l'Eurodac via CIR. Tuttavia, la nostra ricerca ha dimostrato che l'approccio a cascata non è stato effettivamente soppresso. Secondo l'art. 22, l'accesso delle autorità di polizia e di Europol ai dati memorizzati nel CIR sarà semplificato attraverso un processo bifasico: in una prima fase, l'autorità o il funzionario Europol inserirà i dati normalmente utilizzati per accedere al sistema sottostante così da poter ottenere un riferimento al sistema contenente i dati corrispondenti; in una seconda fase, l'autorità o il funzionario Europol dovrà accedere al sistema o ai sistemi in caso di corrispondenza. Con la revisione del Regolamento VIS, l'art. 22 è stato aggiunto all'elenco dei requisiti esistenti per consentire l'accesso al sistema da parte delle forze dell'ordine, cosa che riteniamo positiva in quanto si rafforza l'aspettativa per cui il sistema contiene davvero i dati ricercati. Tuttavia, la Proposta di Regolamento Prüm II prevede l'implementazione di un *router* che consentirà l'interrogazione simultanea delle banche dati degli Stati membri, dei dati Europol e del CIR attraverso l'ESP, e richiede che le autorità designate per l'EES, il VIS e l'ETIAS rispettino l'art. 22. Abbiamo sostenuto che questo potrebbe essere un altro tentativo di aggirare il principio di proporzionalità sopprimendo l'approccio a cascata.

5.3. Abbiamo evidenziato che gli obiettivi dell'interoperabilità devono essere supportati da elevati standard di qualità dei dati che garantiscano risultati affidabili.

Questi standard non dipendono solo dalla fornitura di meccanismi specifici, ma anche dalle circostanze che circondano l'inserimento dei dati nei sistemi e nelle componenti

dell'interoperabilità. I Regolamenti IO prevedono che il formato universale dei messaggi (UMF) e l'archivio centrale di relazioni e statistiche (CRRS) saranno implementati per scopi semantici e statistici. L'elaborazione di dati a fini semantici e statistici non serve solo ad assistere l'attività operativa delle autorità nazionali e dei funzionari dell'Unione, ma anche a presentare nuove proposte legislative.

6. L'interoperabilità e la competenza esterna dell'UE sulla protezione dei dati personali e la libera circolazione di tali dati

6.1. L'interoperabilità faciliterà l'interrogazione rapida, continuata, ed efficiente dei sistemi IT su larga scala dell'UE e le componenti dell'interoperabilità essendo l'ESP la porta d'accesso a una forma globale di interoperabilità.

La comunicazione dei dati personali regolata dall'art. 50 dei Regolamenti IO dovrebbe essere letta in termini di agevolazione dell'identificazione dei nazionali di Paesi terzi i cui dati sono memorizzati nel CIR e, eventualmente, nel MID. Tuttavia, i Regolamenti IO non chiariscono quali tipi di dati saranno effettivamente condivisi.

Abbiamo analizzato l'art. 50 sulla base di un concetto ampio di interoperabilità che comprende sia l'interconnessione delle banche dati straniere con l'infrastruttura dell'Unione sia la capacità di lettura dei dati scambiati da parte di autorità terze. Successivamente, abbiamo notato che l'art. 50 si struttura su tre livelli principali.

- In primo luogo, l'art. 50 fa riferimento ad alcuni dei Regolamenti sui sistemi IT su larga scala sottostanti – vale a dire VIS, EES e ETIAS – ed abbiamo sostenuto che anche SIS, Eurodac e ECRIS-TCN avrebbero dovuto essere previsti dal Regolamento (UE) 2019/818.
- In secondo luogo, l'art. 50 richiama gli arts. 25 e 26 del Regolamento Europol suggerendo, a nostro avviso, che il Sistema di Informazione di Europol (SIE) potrebbe essere interconnesso anche con banche dati straniere. Sebbene non siano dotati di sistemi propri, si presume che anche Eurojust, l'Agenzia EGFC, l'EUAА contribuiranno alla dimensione esterna dell'interoperabilità nella misura in cui queste agenzie concludono accordi e/o intese internazionali attraverso le quali scambiano dati personali con Paesi terzi e organizzazioni internazionali.
- In terzo luogo, l'art. 50 prevede che le banche dati SLTD e TDAWN di Interpol siano interconnesse al CIR tramite l'ESP.

In particolare, l'art. 50 ricorda che il trasferimento o la messa a disposizione dei dati deve rispettare la piramide di strumenti di cui al Capo V RGPD, al Capo V LED e al Capo V EUDPR.

Abbiamo preso nota del fatto che i Paesi terzi o le organizzazioni internazionali potrebbero essere sottoposti a una decisione di adeguatezza della Commissione europea, o no. Quando non c'è una decisione di adeguatezza, abbiamo avvertito che il responsabile del trasferimento dei dati deve assicurare che siano in atto “garanzie adeguate” e, concretamente, che l'individuo abbia a disposizione meccanismi di ricorso appropriati. In alternativa, abbiamo ipotizzato che i dati personali possano essere comunicati perché un accordo amministrativo o un'intesa è in atto tra un ente dell'UE, di un paese terzo o di un'organizzazione internazionale. In tal caso, abbiamo esaminato il mandato di ogni agenzia alla luce dell'*acquis* dell'UE sulla protezione dei dati e i limiti stabiliti dalla dottrina della delega. Come ultima risorsa, abbiamo considerato il fatto che il trasferimento potrebbe essere basato su clausole di deroga – cioè, trasferimenti *ad hoc*. In questo contesto, abbiamo valutato il grado ottimale di interoperabilità per ogni situazione specifica contemplata dall'art. 50 secondo le norme giuridiche internazionali e sovranazionali. Nella misura in cui l'interoperabilità rispetta questi parametri, è lecita e “sostenibile” – i.e., coerente – nei confronti dell'azione interna dell'UE. Tuttavia, quest'ultima potrebbe richiedere ulteriori garanzie che riteniamo necessarie per salvaguardare i dati personali quando questi vengono trasferiti da/verso terzi.

6.2. La comunicazione di dati personali a Paesi terzi, all'Organizzazione Internazionale per le Migrazioni (OIM), all'Agenzia ONU per i Rifugiati (UNHCR) e al Comitato Internazionale della Croce Rossa (CICR) per il ritorno dei migranti illegali/irregolari, e la comunicazione di dati personali ai fini della PJCCM dovrebbe essere limitata a trasferimenti *ad hoc*, sulla base delle clausole derogatorie.

Anzitutto, abbiamo notato che il trasferimento di dati personali basato su accordi di riammissione, che si considerano “appropriati”, è discutibile se si analizza come la clausola inserita in questi accordi manchi di elementi essenziali in materia protezione dei dati personali che garantirebbero la loro esecutività. Incoraggiamo i co-legislatori a rafforzare le garanzie previste da questa clausola e, più in generale, a chiarire quando possiamo dire che il responsabile del trattamento dispone degli strumenti necessari per garantire che il trasferimento compia con la previsione di “garanzie adeguate”. Posto che il trasferimento di dati personali all'OIM, l'UNHCR e il CICR non è regolato né da una decisione di adeguatezza, né da garanzie adeguate – i.e., un accordo internazionale/amministrativo o un'intesa –, abbiamo sostenuto che l'interoperabilità dovrebbe essere mantenuta solo a livello di trasferimenti di dati *ad hoc* tra le parti. Anche il trasferimento di dati ai fini della PJCCM è relegato a specifiche clausole

derogatorie che permettono la comunicazione di dati personali «in casi eccezionali di urgenza», per cui l'interconnessione deve limitarsi a la messa a disposizione di dati in modo puntuale.

6.3. In assenza di una decisione di adeguatezza su Interpol, l'Accordo di Cooperazione UE-Interpol consentirebbe l'interoperabilità dei sistemi IT su larga scala e delle componenti dell'Unione con le banche dati SLTD e TDAWN. Tuttavia, la negoziazione di questo Accordo di Cooperazione deve essere criticata, in quanto vi è una forte evidenza che non tutti i Paesi membri di Interpol condividono i principi fondanti dell'Unione, ovvero la libertà, la democrazia e il rispetto dei diritti umani, delle libertà fondamentali e dello Stato di diritto.

L'imminente Accordo di Cooperazione UE-Interpol vuole: assicurare l'accesso diretto e reciproco alle rispettive banche dati di Europol e di Interpol; interconnettere i sistemi IT su larga scala – specialmente l'ETIAS – con i database SLTD e TDAWN di Interpol, e garantire a Europol, all'Agenzia EGFC, a Eurojust e alla Procura europea (EPPO) l'accesso diretto alle banche dati di Interpol. Prima di concludere un tale accordo, è necessario prendere in considerazione le seguenti questioni:

- primo, la portata dell'Accordo previsto deve essere ulteriormente esaminata finché non è si chiarisce la questione della soggettività internazionale di Interpol;
- secondo, nella causa *WS c Bundesrepublik Deutschland*, la CGUE non si è pronunciata sul fatto che questa organizzazione garantisca un livello adeguato di protezione dei dati personali rispetto all'UE, e nessuna decisione sul suo livello di protezione è stata adottata finora;
- terzo, l'interconnessione delle banche dati Interpol con l'infrastruttura dell'interoperabilità non dovrebbe, in nessun caso, rivelare le notifiche rosse al proprietario della segnalazione, il che richiede la modifica delle Regole sul trattamento dei dati di Interpol, e
- quarto, l'Accordo di Cooperazione rischia di sconfinare nella PESC, dove non esiste una normativa che regola il trasferimento di dati personali e non è coerente con la sua proiezione interna.

In ogni caso, se l'Accordo di Cooperazione annunciato mira a garantire la consultazione sistematica delle banche dati di Interpol, questo non potrà essere una dichiarazione di principi, ma deve rispettare il requisito di “esecutività” che assicura diritti effettivi alle persone interessate. In caso contrario, la comunicazione di dati personali dovrebbe essere considerata regolata da accordi amministrativi o clausole di deroga.

6.4. Il SIE non migrerà nell'infrastruttura dell'interoperabilità, ma sarà interoperabile con essa e potrà collegarsi a sistemi di terzi anche sulla base degli accordi internazionali e amministrativi concluse da Europol. Occorre chiarire se le intese di lavoro rispettano il divieto di trasferimento sistematico, massivo o strutturale dei dati personali, dal momento che consentono “complessi di trasferimento”.

Il SIE non migrerà nell'infrastruttura dell'interoperabilità, ma diventerà interoperabile con essa e potrebbe creare un ponte anche con i sistemi dei partner stranieri. Il SIE memorizza diversi tipi di dati personali, anche sensibili, appartenenti a persone sospettate di aver commesso reati, per i quali Europol è competente, nonché appartenenti alle vittime. Inoltre, Europol filtra i dati di persone che non rientrano nel suo mandato, avvicinando sempre più ad un'agenzia d'intelligence. Anche se la proposta della Commissione europea secondo la quale l'agenzia avrebbe potuto inserire segnalazioni nel SIS è stata definitivamente respinta, quest'agenzia ha accesso a tutti i sistemi IT su larga scala.

Europol ha sviluppato la sua attività esterna sulla base di accordi operativi attraverso i quali poteva scambiare dati personali con autorità straniere. La legittimità di questi accordi è stata seriamente messa in discussione alla luce dello stretto coinvolgimento del Consiglio dell'UE, che risultava vincolare l'Unione piuttosto che l'agenzia. Il nuovo Regolamento ha eliminato gli accordi di cooperazione, ma a Europol è stata delegata la conclusione di accordi di lavoro con i quali continua a scambiare dati personali in modo contraddittorio: gli accordi di lavoro non sono una base giuridica valida per il trasferimento di dati personali ma prevedono la possibilità di trasferirli comunque. Il Regolamento Europol prevede che, in assenza di una decisione di adeguatezza, i dati personali possano essere trasferiti mediante un accordo internazionale concluso dall'UE ai sensi dell'articolo 218 del TFUE. Il GEPD ha ricordato che tale accordo dovrebbe essere sostenuto dall'art. 16(2) del TFUE e ha messo in dubbio l'impegno di alcuni Paesi terzi con i quali sono già stati avviati negoziati nel settore dei diritti umani. Sebbene il Regolamento Europol stabilisca che le clausole di deroga non possono implicare un trasferimento sistematico, massiccio o strutturale di dati, esso delega anche al Direttore Esecutivo la competenza di autorizzare serie di trasferimenti per un periodo non superiore ad un anno «tenendo conto dell'esistenza di garanzie adeguate per quanto riguarda la protezione della vita privata e dei diritti e delle libertà fondamentali delle persone». Non è chiaro se i «complessi di trasferimenti» rispettino sempre il limite della proibizione di trasferimenti di dati sistematici, massicci o strutturali.

6.5. A differenza di Europol, Eurojust ha accesso a due dei sei sistemi IT su larga scala: le segnalazioni SIS per la cooperazione di polizia e giudiziaria in materia penale e l'ECRIS-TCN. Ad oggi non è stata prevista nessuna interoperabilità tra il CMS e i sistemi IT su larga scala dell'Unione o tra il CMS e le banche dati estere. Tuttavia, la situazione potrebbe cambiare in un futuro prossimo.

Il CMS di Eurojust conserva varie categorie di dati personali, compresi quelli sensibili, rispettivamente nell'Indice e nel TWF. Il regime applicabile al trattamento dei dati personali da parte di Eurojust cambia a seconda che si tratti di dati relativi a casi per cui l'agenzia è competente o no. Il primo è legato alle attività operative di Eurojust e riguarda le indagini o i procedimenti penali, nonché i testimoni o le vittime; il secondo, invece, riguarda i membri del personale e le informazioni amministrative.

Eurojust è designata come punto di contatto per i Paesi terzi e le organizzazioni internazionali che chiedono agli Stati membri di accedere al casellario giudiziario di un nazionale di un Paese terzo. Se durante la ricerca nell' ECRIS-TCN l'agenzia scopre che un nazionale di un Paese terzo è stato condannato penalmente in uno Stato membro, deve informare il Paese terzo affinché questo si rivolga a tale Stato membro se, e solo se, quest'ultimo ha dato il suo consenso. La possibilità per Eurojust di ricevere richieste di cooperazione giudiziaria trasforma l'agenzia in un vero catalizzatore in materia di cooperazione giudiziaria penale internazionale.

Analogamente a Europol, Eurojust può concludere accordi di cooperazione con Paesi terzi e organizzazioni – sia internazionali che nazionali – che comprendono il trasferimento di dati personali a fini operativi. La loro conclusione seguiva una lista di Paesi e organizzazioni internazionali approvata dal Collegio di Eurojust che era sottoposta all'approvazione del Consiglio. Questi elementi ci portano a concludere che gli accordi di cooperazione devono essere considerati come accordi esecutivi conclusi per conto dell'UE senza che ci sia stata una vera delega in conformità con sentenza *Meroni* e seguenti. In ogni caso, con il nuovo Regolamento gli accordi di cooperazione sono stati soppressi e ora l'agenzia può trasferire dati personali in base a: una decisione di adeguatezza, o una salvaguardia adeguata, o una clausola di deroga specifica; un accordo di cooperazione concluso prima del 12 dicembre 2019, o un accordo internazionale tra l'UE e il Paese terzo o l'organizzazione internazionale ai sensi dell'art. 218 del TFUE. Di conseguenza, nel caso di Eurojust, lo scambio di dati personali dall'UE ai Paesi terzi e alle organizzazioni internazionali non può essere canalizzato attraverso *soft law* o accordi di lavoro, il che è in linea con l'EUDPR e (apparentemente) con il Regolamento

Europol. Tuttavia, il Regolamento Eurojust rende sicuri due strumenti rilevanti: in primo luogo, la posizione comune 2005/69/GAI del Consiglio sullo scambio di dati personali con Interpol; in secondo luogo, la decisione 2007/533/GAI del Consiglio sull'istituzione, l'esercizio e l'uso del SIS II con Interpol.

6.6. L'Agenzia EGFC è il secondo organismo più importante per l'interoperabilità, dato che ha accesso a quattro su sei sistemi IT su larga scala, soprattutto per finalità statistiche, mentre l'Unità centrale ETIAS non ha accesso ad uno soltanto. L'Agenzia EGFC trasferisce dati personali a terzi attraverso intese di lavoro o accordi di status: i primi sono strumenti *soft* che mancano di sostegno democratico; i secondi sono privi di «garanzie essenziali per la protezione dei dati».

Dato che il mandato dell'Agenzia EGFC copre sia attività nel campo della gestione delle migrazioni – soprattutto in materia di ritorno dei migranti che entrano illegalmente nell'UE – sia nel campo della criminalità grave con dimensione transfrontaliera, è difficile discernere quale regime di protezione dei dati sia applicabile alle attività di questa agenzia. L'Agenzia EGFC ha aumentato esponenzialmente i suoi compiti operativi dopo la crisi umanitaria del 2015 e lo stesso vale per il trattamento delle informazioni. Secondo il Regolamento dell'Agenzia EGFC del 2019, gli Stati membri sono obbligati a condividere le loro informazioni con essa e sono tenuti a inserire legittimamente informazioni accurate e aggiornate nelle banche dati europee. L'agenzia elabora i dati personali nel quadro di operazioni congiunte, progetti pilota e interventi rapidi per il rimpatrio dei migranti illegali e potrebbe combinare questi dati con informazioni sul trasporto sospetto e/o rilevato. L'agenzia “controlla” anche i nazionali di Paesi terzi dopo lo sbarco in frontiera e tratta i dati personali relativi a persone rispetto alle quali le autorità competenti degli Stati membri sospettano, per motivi ragionevoli, di essere coinvolte in attività criminali transfrontaliere, nel facilitare attività di migrazione illegale o in attività di traffico di esseri umani. Inoltre, le squadre dell'Agenzia EGFC hanno accesso a sistemi IT su larga scala nell'esecuzione dei loro compiti nel territorio degli Stati membri. Solo i Regolamenti (UE) 2018/1861 e 2018/1862 vietano espressamente l'interconnessione del SIS «[...] a qualsiasi sistema di raccolta ed elaborazione dati gestito dalle squadre di cui al paragrafo 1 o dall'Agenzia europea della guardia di frontiera e costiera, né i dati del SIS a cui hanno accesso tali squadre sono trasferiti a un tale sistema».

L'Agenzia EGFC ha concluso intese di lavoro non vincolanti con Paesi terzi e organizzazioni internazionali, che sono adottati dal suo consiglio di amministrazione a maggioranza assoluta, previa approvazione della Commissione europea e dopo aver informato il Parlamento europeo e il Consiglio dell'UE. La maggior parte degli accordi di lavoro non specifica se i “dati personali

operativi” possono essere scambiati sulla base di tali accordi non vincolanti. È il Regolamento dell'Agenzia EGFC del 2019 che li considera una base giuridica valida per trasferire i dati personali in assenza di un accordo di status, o nel caso in cui l'accordo di status non miri a regolare il trattamento dei dati personali o non contenga garanzie complete e sufficienti per la protezione dei dati. Gli accordi di status coprono tutti gli aspetti pertinenti necessari per svolgere il mandato dell'agenzia, comprese disposizioni sullo scambio di informazioni e il trasferimento di dati personali, a cui il GEPD dovrebbe acconsentire. Inoltre, gli accordi di status prevedono una clausola sulla protezione dei dati personali che specifica che, mentre il Paese terzo è soggetto alla sua legislazione nazionale, le squadre dell'Agenzia EGFC rispondono al EUDPR e i funzionari degli Stati membri rispondono al GDPR e alla LED. Tuttavia, il GEPD ha affermato che il modello di status è privo di «garanzie essenziali per la protezione dei dati» e che avrebbe dovuto essere stato elaborato più dettagliatamente per conformarsi al diritto dell'UE.

6.7. Non è chiaro in quali termini la EUAA possa avere accesso ai sistemi IT su larga scala e alle componenti dell'interoperabilità, dato che il suo Regolamento garantisce al personale l'accesso sia alle banche dati degli Stati membri che a quelle europee. L'EUAA può trasferire i dati personali a Paesi terzi e organizzazioni internazionali attraverso accordi di lavoro che non garantiscono «diritti esecutivi ed effettivi agli interessati».

Il mandato della EUAA è stato recentemente riformato per permettere all'agenzia di scambiare e analizzare informazioni, e per imporre agli Stati membri di cooperare con il suo personale. L'EUAA può elaborare i dati personali relativi alle domande di protezione internazionale presentate alle amministrazioni e alle autorità nazionali, e agli sviluppi nazionali e legali in materia d'asilo, comprese le banche dati della giurisprudenza rilevante. Anche se l'EUAA non è dotata di un proprio sistema IT, si prevede che ne svilupperà uno con l'aiuto di eu-LISA. Oltre all'elaborazione del Sistema di Allarme Rapido e di Preparazione basato su dati statistici, i gruppi di supporto per l'asilo trattano dati personali quando assistono gli Stati membri nell'identificazione e nella registrazione di nazionali di Paesi terzi e nell'ambito del reinsediamento.

L'EUAA è stata delegata la competenza per concludere accordi di lavoro con Paesi terzi che sono in ultima istanza sottoposti all'approvazione della Commissione europea – mentre il Parlamento europeo e il Consiglio devono essere informati prima della loro conclusione. Questi accordi incanalano il trasferimento di dati personali verso Paesi terzi e organizzazioni internazionali – per esempio, all'UNHCR e all'OIM – ai fini del reinsediamento: in assenza di

una decisione di adeguatezza, o di uno strumento giuridicamente vincolante ed esecutivo, queste intese amministrative permettono lo scambio di dati personali con partner stranieri a livello “operativo”. Come nel caso dell’Agenzia EGFC, occorre avvertire che il trasferimento di dati personali tramite accordi non vincolanti non garantisce l’esecutività e l’effettiva protezione dei diritti degli interessati. Inoltre, il Regolamento EUAA non prevede la necessità di alcuna autorizzazione da parte del GEPD, come dovrebbe in caso all’art. 48(3)(b) del EUDPR.

Bibliography

Literature

Book

- Alan Dashwood and Joni Helikoski, *The General Law of E.C. External Relations*, London, Sweet/Maxwell, 2000.
- Alan Dashwood, Michael Dougan, Barry Rodger, Eleanor Spaventa, and Derrick Wyatt, *Wyatt and Dashwood's European Union Law*, Oregon, Hart Publishing, 2011.
- Alan F. Westin, *Privacy and Freedom*, New York, Atheneum, 1970.
- Alessandra Annoni and Arianna Tiene, *Minori e privacy. La tutela dei dati personali dei bambini e degli adolescenti alla luce del Regolamento (UE) 2016/679*, Ferrara, Jovene, 2019.
- Alessandra Annoni and Francesco Salerno, *La tutela internazionale della persona umana nei conflitti armati*, Cacucci Editore, Bari, 2019.
- Ana Salinas De Frías, *La Protección de los Derechos Fundamentales en la Unión Europea*, Granada, Comares, 2000.
- Andreia Ribeiro and Vania Baldi, *The Potential Role of Digital Technologies in the Context of Forced Displacement*, Cham, Springer International Publishing, 2018.
- Anna Fiodorova, *Information Exchange and EU Law Enforcement*, London, Routledge, 2018.
- Annegret Engel, *The Choice of Legal Basis for Acts of the European Union: Competence Overlaps, Institutional Preferences, and Legal Basis Litigation*, Cardiff, Springer, 2018.
- Bald de Vries, Jet Tigchelaar, Tina van der Linden, and Ton Hol, *Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen. Disciplinegroep Rechtstheorie, Departement Rechtsgeleerdheid*, University of Utrecht, 2007.
- Brendan Van Alsenoy, *Data protection Law in the EU: Roles, Responsibilities and Liability*, Cambridge, Intersentia, 2019.
- Cecilia Corsi, *Agenzia e agenzie: una nuova categoria amministrativa?*, Torino, Giappichelli Editore, 2005.
- Christopher David and Nicholas Hearn, *A Practical Guide to INTERPOL and Red Notices*, Great Britain, Bloomsbury, 2018.
- Chris Reed, *Making Laws for Cyberspace*, Oxford, Oxford University Press, 2012.

- Christopher Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford, Oxford University Press, 2013.
- Cláudia Faria, *The Dublin Convention on Asylum: between reality and aspirations*, Maastricht, European Institute of Public Administration, 2001.
- Clotilde Marinho, *The Dublin Convention on Asylum: its essence, implementation and prospects*, Maastricht, European Institute of Public Administration, 2000.
- Colin J. Bennett and Rebecca Grant, *Visions of Privacy: Policy Choices for the Digital Age*, Toronto, University of Toronto Press, 1999.
- Costa Olivier and Brack Nathali, *How the EU really works*, New York, Routledge, 2019.
- Cristina Blasi Casagran, *Global Data Protection in the Field of Law Enforcement: An EU perspective*, Abingdon, Routledge Research in EU Law, 2017.
- David Fernández Rojo, *EU Migration Agencies: The Operation and Cooperation of FRONTEX, EASO and EUROPOL*, Cheltenham, Edward Elgar Publishing, 2021.
- David O' Keffe and Henry G Schermers, *Mixed Agreements*, Deventer, Kluwer, 1983.
- Dinah Shelton, *Remedies in international human rights law*, Oxford, Oxford University Press, 2015.
- Edoardo Chiti, *Le agenzie europee*, Padova, CEDAM, 2002.
- Edward Snowden translated by Esther Cruz Santaella, *Vigilancia Permanente*, Barcelona, Planeta, 2019.
- Eljalill Tauschinsky and Wolfgang Weiß, *The Legislative Choice Between Delegated and Implementing Acts in EU Law: Walking in a Labyrinth*, Cheltenham, Edgar Elgar Publishing, 2018.
- Enrique Pérez Luño, *La tercera generación de Derechos Humanos*, Pamplona, Aranzadi, 2006.
- Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *International Law as Law of the European Union*, Leiden, Martinus Nijhoff Publishers, 2012.
- Evelien Brouwer, *Digital borders and real rights: effective remedies for third-country nationals in the Schengen Information System*, Leiden, Martinus Nijhoff Publishers, 2008.
- Francesco Contini and Giovan Francesco Lanzara, *The Circulation of Agency in E-Justice: Interoperability and Infrastructures for European Transborder Judicial Proceedings*, Dordrecht Heidelberg/New York/London, Springer, 2014.
- Francesco Salerno, *Diritto internazionale: Principi e norme*, Padova, 2020.

- Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Luxembourg, Springer, 2012.
- Frédéric Mégret and Philip Alston, *The United Nations and Human Rights: A critical appraisal*, Oxford, Oxford University Press, 2020.
- Geert De Baere, *Constitutional Principles of EU External Relations*, Oxford, Studies in European Law, 2008.
- Giorgio Gaja and Adelina Adina, *Introduzione al Diritto dell'Unione europea*, Urbino, Editori Laterza, 2020.
- Giovanni Barrocu, *La cooperazione investigativa in ambito europeo: Da Eurojust all'ordine di indagine*, Milano, CEDAM, 2017.
- Gloria Fernández Arribas, *Las capacidades de la Unión Europea como sujeto de Derecho Internacional*, Granada, Educatori, 2010.
- Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Switzerland, Springer, 2014.
- Henry G. Schermers and Niels M. Blokker, *International Institutional Law: Unity within Diversity*, Boston, Martinus Nijhoff Publishers, 2011.
- Herwig C.H. Hofmann, Gerard C. Rowe, and Alexander H. Türk, *Administrative law and policy of the European Union*, Oxford, Oxford University Press, 2013.
- Hielke Hijmans, *The European Union as Guardian of Internet Privacy*, Switzerland, Springer, 2016.
- Isabel Hernández Gómez, *Sistemas internacionales de Derechos humanos*, Madrid, Dykinson, 2001.
- Jacopo Alberti, *Le Agenzie dell'Unione Europea*, Milano, Giuffré, 2018.
- Jacques Delors, *Subsidiarity: The Challenge of Change. Proceedings of the Jacques Delors Colloquium*, Maastricht, European Institute of Public Administration, 1991.
- James C. Hathaway, *The rights of disputes under international law*, Cambridge, Cambridge University Press, 2018.
- James Waldo, Herbert Lin, and Lynette I Millett, *Engaging privacy and information technology in a digital age*, Washington, National Academies Press, 2007.
- Jan Wouters, André Nollkaemper, and Erika de Wet, *The Europeanisation of International Law: The Status of International Law in the EU and its Member States*, The Hague, TMC Asser Press, 2008.

- Javier Valls Prieto, *Problemas jurídicos penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial*, Madrid, Dykinson, 2017.

- John Palfrey and Urs Gasser, *Interop: The Promise and Perils of Highly Interconnected Systems*, US, Basic Books, 2012.

- Jonathan P. Aus, *Supranational governance in an “area of freedom, security and justice”: Eurodac and the politics of biometric control*, Sussex, Sussex European Institute, 2003.

- José Antonio Pastor Ridruejo, *Curso de Derecho Internacional Público y Relaciones Internacionales*, Madrid, Tecnos, 2021.

- Juan Santos Vara, *La gestión de las fronteras exteriores de la UE Los nuevos poderes de la Agencia Frontex*, Valencia, Tirant Lo Blanch, 2021.

- Katarzyna Granat, *The principle of subsidiarity and its enforcement in the EU Legal Order: The Role of National Parliaments in the Early Warning System*, Oxford, Hart Publishing, 2018.

- Lucas J. Ruiz Díaz, *La acción exterior de la Unión Europea contra el Crimen Organizado Transnacional: Aspectos internos y dinámicas externas del discurso securitario*, Madrid, Tecnos, 2017.

- Luis Miguel Hinojosa Martínez, *El reparto de competencias entre la Unión Europea y sus Estados miembros*, Valencia, Tirant Lo Blanch, 2006.

- Manfred Nowak, *The International Covenant on Civil and Political Rights*, Bilbao, HumanitarianNet, 2009.

- Manuel Díez de Velasco Vallejo, *Las Organizaciones Internacionales*, Madrid, Tecnos, 2010.

- Manuel Pombo, *La realidad migratoria y las políticas migratorias: la organización internacional para las migraciones*, Madrid, Dykinson, 2012.

- María del Carmen Muñoz Rodríguez, *Democracia y derechos humanos en la acción exterior de la Unión Europea*, Madrid, Reus, 2010.

- María Esther Jordana Santiago, *El proceso de institucionalización de Eurojust y su contribución al desarrollo de un modelo de cooperación judicial penal de la Unión Europea*, Madrid, Marcial Pons, 2018.

- María Eugenia Rodríguez Palop, *La nueva generación de derechos humanos: origen y justificación*, Madrid, Dykinson, 2018.

- María Mercedes Candela Soriano, *Los Derechos Humanos, la democracia y el estado de derecho en la acción exterior de la Unión Europea: Evolución, actores, Instrumentos y Ejecución*, Madrid, Dykinson, 2006.
- María Rosa Ripollés Serrano, *Constituciones de los 27 Estados miembros de la Unión Europea*, Madrid, Congreso de los Diputados, 2010.
- Marta Simoncini, *Administrative Regulation Beyond the Non-Delegation Doctrine: A study on EU Agencies*, Oxford, Hart Publishing, 2018.
- Martín y Pérez de Nanclares, *El Sistema de competencias de la Comunidad Europea*, Madrid, McGraw-Hill, 1997.
- Megan Bradley, *The international organization for migration: challenges and complexities of a rising humanitarian actor*, London: Routledge, 2015.
- Merijn Chamon, *EU Agencies: Legal and Political Limits to the Transformation of the EU Administration*, Oxford, Oxford Studies in European Law, 2016.
- Merijn Chamon, Herwig C.H. Hofmann, and Ellen Vos, *The External Dimension of EU Agencies and Bodies: Law and Policy*, Cheltenham, Edward Elgar Publishing, 2019.
- Myriam Benlolo-Carabot, Ulas Candas, and Eglantine Cujo, *Union Européenne et droit international: En l'honneur de Patrick Daillier*, Paris, Editions Pedone, 2012.
- Nisuke Ando, *Towards implementing Universal Human Rights*, Leiden/Boston, Martinus Nijhoff Publishers, 2004.
- Olivier de Schutter, *International Human Rights Law*, Cambridge, Cambridge University Press, 2017.
- Oriol Casanovas and Ángel J. Rodrigo Hernández, *Compendio de Derecho Internacional Público*, Madrid, Tecnos, 2020.
- Orla Lynskey, *The Foundations of EU Data Protection Law*, Oxford, Oxford Studies in European Law, 2015.
- Paloma Llana González, *Identidad digital*, Madrid, Wolters Kluwer, 2021.
- Paolo Picone, *Comunità internazionale e obblighi «erga omnes»*, Napoli, Jovene Editore, 2013.
- Paul Craig and Gráinne De Búrca, *EU Law: Text, Cases and Materials*, Oxford, Oxford University Press, 2011.
- Paul Craig, *EU Administrative Law*, Oxford, Oxford University Press, 2018.
- Paula García Andrade, *La acción exterior de la Unión Europea en la materia migratoria: Un problema de reparto de competencias*, Valencia, Tirant Lo Blanch, 2015.

- Philip Alston and Ryan Goodman, *International Human Rights. The successor to international human rights in context: law, politics and morals*, Oxford, Oxford University Press, 2013.

- Philippe Léger, *Union Européenne: Commentaire Article par Article des Traités UE et CE*, Helbig/Lichtenhahn, Dalloz, 2000.

- Piet Eeckhout, *EU External Relations Law*, Oxford, Oxford University Press, 2012.

- Pieter Boeles, Maarten Den Heijer, Gerrie Lodder, Kees Wouters, *European Migration Law*, Cambridge, Intersentia, 2014.

- Rafael Marin Aís, *La participación de la Unión Europea en tratados internacionales para la protección de los derechos humanos*, Madrid, Tecnos, 2013.

- Rebekah Dowd, *The Birth of Digital Human Rights: Digitized Data Governance as a Human Rights Issue in the EU*, Cham, Palgrave Macmillan, 2022.

- Robert Schütze, *European Union Law*, Cambridge, Cambridge University Press, 2018.

- Roberta Mangianu, *Frontex and Non-Refoulement: The International Responsibility of the EU*, Cambridge, Cambridge Studies in European Law and Policy, 2016.

- Roberto Adam and Antonio Tizzano, *Lineamenti di Diritto dell'Unione Europea*, Torino, Giappichelli Editore, 2022.

- Russell Buchan, *Cyber Espionage and International Law*, Oxford, Hart Publishing, 2018.

- Rutsel Silvestre J. Martha, *The Legal Foundations of INTERPOL*, Oxford/Portland/Oregon, Hart Publishing, 2010.

- Sarah Deardorff Miller, *UNHCR as a surrogate state: protracted refugee situations*, London/New York, Routledge/Taylor and Francis Group, 2018.

- Sergio Carrera, *Implementation of EU Readmission Agreements Identity Determination Dilemmas and the Blurring of Rights*, Cham, Springer International Publishing, 2016.

- Stefania Carnevale, Serena Forlati, and Orsetta Giolo, *Redefining Organised Crime: A Challenge for the European Union?*, Oxford, Hart Publishing, 2017.

- Stephan Kabera Karanja, *Transparency and proportionality in the Schengen Information System and border control co-operation*, Leiden, Nijhoff, 2008.

- Steve Peers, *EU Justice and Home Affairs Law, Volume I: EU Immigration and Asylum Law*, Oxford, Oxford EU Law Library, 2016.

- Steve Peers, *EU Justice and Home Affairs Law, Volume II: EU Criminal Law, Policing, and Civil Law*, Oxford, Oxford EU Law Library, 2016.

- Steven Greer, Janneke Gerards, and Rose Slowe, *Human Rights in the Council of Europe and the European Union: Achievements, Trends, and Challenges*, Cambridge, Cambridge Studies in European Law and Policy, 2018.
- Teresa Fajardo del Castillo, *La Diplomacia del Clima de la Unión Europea: La Acción Exterior sobre Cambio Climático y el Pacto Verde Mundial*, Madrid, Reus, 2021.
- Teresa Fajardo del Castillo, *La política exterior de la Unión Europea en materia de medio ambiente*, Madrid, Tecnos, 2005.
- Terri Givens, Gary P. Freeman, and David L. Leal, *Immigration Policy and Security*, New York, Routledge, 2008.
- Theodor Meron, *International law in the Age of Human Rights: General Course on Public International Law*, Leiden/Boston, Martinus Nijhoff Publishers, 2003, pp. 9-490.
- Valentín Bou Franch and Mireya Castillo Daudí, *Derecho internacional de los derechos humanos y Derecho internacional humanitario*, Valencia, Tirant Lo Blanch, 2014.
- Vendelin Hreblay, *La libre circulation des personnes: les accords Schengen*, Paris, Les Éditions G. Crès et Cie., 1994.
- Vendelin Hreblay, *Les accords de Schengen: origine, fonctionnement et avenir*, Brussels, Bruylant, 1998.
- William A. Schabas, *The Customary International Law of Human Rights*, Oxford, Oxford University Press, 2021.
- Yves Pascouau, *La politique migratoire de l'Union Européenne: De Schengen à Lisbonne*, Paris, L.G.D.J., 2010.

Book chapter

- A. G. Toth, "A legal Analysis of Subsidiarity", in David O'Keefe and Patrick M. Twomey, *Legal issues of Maastricht Treaty*, London, Chancery, 1994, pp. 37-48.
- Alan Dashwood, "Mixity in the Era of the Treaty of Lisbon", in Christophe Hillion and Panos Koutrakos, *Mixed Agreements Revisited: The EU and its Member States in the World*, Oxford, Hart Publishing, 2010, pp. 351-366.
- Alberto Giovanetti Ramos, "Inmigrantes en situación irregular y la Organización Internacional para las Migraciones", in Angel G. Chuenca Sancho, *Derechos Humanos, inmigrantes en situación irregular y Unión Europea*, Valladolid, Lex Nova, 2010, pp. 97-111.
- Alessandra Gianelli, "Customary International Law in the European Union", in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *International Law as Law of the European Union*, Leiden, Martinus Nijhoff Publishers, 2012, pp. 93-110.

- Alexandros Kargopoulos, "Fundamental rights, national identity and EU criminal law", in Valsamis Mitsilegas, Maria Bergstrom, and Theodora Konstadinides, *Research Handbook on EU Criminal Law*, Cheltenham, Edward Elgar Publishing, 2016, pp. 125-147.

- Alicia Cebado Romero, "La peculiaridad de la Acción Exterior de la Unión Europea", in Antonio Remiro Brotons and Irene Blázquez Navarro, *El Futuro de la Acción Exterior de la Unión Europea*, Valencia, Tirant Lo Blanch, 2006, pp. 73-100.

- Allan Rosas, "International Responsibility of the EU and the European Court of Justice", in Malcolm Evans and Panos Koutrakos, *The international responsibility of the European Union*, Oregon, Hart Publishing, 2013, pp. 139-261.

- Ana Gascón Marcén, "La Unión Europea y los convenios internacionales elaborados en el marco del Consejo de Europa", in Paula García Andrade, *Interacciones entre el Derecho de la Unión Europea y el Derecho internacional público*, Valencia, Tirant lo Blanch (forthcoming).

- Andrea Ott, "The EU Commission's administrative agreements: "delegated treaty-making" in between delegated and implementing rule-making", in Eljalil Tauschinsky and Wolfgang Weiß, *The Legislative Choice Between Delegated and Implementing Acts in EU Law: Walking in a Labyrinth*, Cheltenham, Edgar Elgar Publishing, 2018, pp. 200-232.

- Andrea Ott, Ellen Vos, and Florin Coman-Kund, "European Agencies on the Global Scene: EU an International Law Perspectives", in Michelle Everson, Cosimo Monda, and Ellen Vos, *European Agencies in between Institutions and Member States*, The Netherlands, Kluwer Law International BV, 2014, pp. 87-122.

- Andreas S. Kolb, "The "Responsibility While Protecting": A Recent Twist in the Evolution of the "Responsibility to Protect"", in Norman WeißJean-Marc Thouvenin, *The Influence of Human Rights on International Law*, Cham, Springer, pp. 79-91.

- Andrew Butterfield and John Szymanski, "information technology, n.", in Butterfield and John Szymanski, *A Dictionary of Electronics and Electrical Engineering*, Oxford, Oxford University Press.

- Andrew Butterfield, Gerard Ekembe Ngond, and Anne Kerr, "automate, v.", in Andrew Butterfield, Gerard Ekembe Ngond, and Anne Kerr, *A Dictionary of Computer Science*, Oxford, Oxford University Press.

- Andrew Butterfield, Gerard Ekembe Ngondi, and Anne Kerr, "Interoperability", in Andrew Butterfield, Gerard Ekembe Ngondi, and Anne Kerr, *Dictionary of Computer Science*, Oxford, Oxford University Press, 2016, available at www.oxfordreference.com.

- Angela Ward, “Article 51 – Field of Application”, in Tamara Hervey, Jeff Kenner, and Angela Ward, *The EU Charter of Fundamental Rights: A Commentary*, Oregon, Hart Publishing, 2014, pp. 1413-1454.
- Anne Peters “The position of International Law Within the European Community Legal Order”, *German Yearbook of International Law*, No. 9, Vol. 40, 1997, pp. 34-35.
- Antonello Tancredi, “On the Absence of Direct Effect of the WTO Dispute Settlement Body’s Decisions in the EU Legal Order,”, in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *International Law as Law of the European Union*, Leiden, Martinus Nijhoff Publishers, 2012, pp. 249-268.
- Antonio Pastor Palomar, “Efectos de los Acuerdos internacionales en el derecho de la UE: práctica reciente y perspectiva desde España”, in José María Beneyto Pérez, *Tratado de Derecho y Políticas de la Unión Europea, Tomo IX: Acción Exterior de la UE*, Navarra, Thomson Reuters Aranzadi, 2017, pp. 81-132.
- Araceli Mangas Martín, “Las competencias de la Unión Europea”, in Araceli Mangas Martín and Diego Javier Liñán Nogueras, *Instituciones y Derecho de la Unión Europea*, Madrid, Tecnos, 2020, on-line resource.
- Augusto J. Piqueras García, “Legalidad y legitimidad en la actividad legislativa de la Unión europea”, in Diego Javier Liñán Nogueras and Pablo Jesús Martín Rodríguez, *Estado de Derecho y Unión Europea*, Madrid, Tecnos, 2018, pp. 313-344.
- Austin Sarat, “Whither Privacy? An Introduction”, in Austin Sarat, *A World Without Privacy: What Law can and Should Do?*, New York, Cambridge University Press, 2015, pp. 1-32.
- Beatrice I. Bonafé, “Direct effect of International Agreements in the EU Legal Order: Does it Depend on the Existence of an International Dispute Settlement Mechanism?”, in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *International Law as Law of the European Union*, Leiden, Martinus Nijhoff Publishers, 2012, pp. 229-28.
- Bernard Kasperek, “Complementing Schengen: The Dublin System and the European Border and Migration Regime”, in Bauder Harald, and Matheis Christian, *Migration Policy and Practice. Migration, Diasporas and Citizenship*, London, Palgrave Macmillan, 2016, pp. 59-78.
- Brigitta Kuster, “How to Liquefy a Body on the Move: Eurodac and the Making of the European Digital Border”, in Raphael Bossong, and Helena Carrapico, *EU Borders and Shifting Internal Security*, Cham, Springer, pp. 45-63.

- Bruno de Witte, “A competence to protect: The pursuit of non-market aims through internal market legislation”, in Philippe Syrpis, *The Judiciary, the Legislature and the EU Internal Market*, Cambridge, Cambridge University Press, 2012, pp. 25-48.

- Bruno de Witte, “Exclusive Member States Competences – Is there such a thing?”, in Sacha Garben and Inge Govaere, *The division of competences between the EU and the member States*, Oxford, Hart Publishing, 2017, pp. 59-73.

- Cécile de Terwangne, “Privacy and data protection in Europe: Council of Europe’s Convention+ and the European Union’s GDPR”, in Gloria González Fuster, Rosamunde Van Berkel, and Paul De Hert, *Research Handbook on Privacy and Data Protection Law: Values, Norms, and Global Politics*, Cheltenham/Northampton, Edward Elgar Publishing, 2022, pp. 10-35.

- Christiaan Timmermans, “Opening Remarks – Evolution of Mixity Since the Leiden 1982 Conference”, in Christophe Hillion and Panos Koutrakos, *Mixed Agreements Revisited: The EU and its Member States in the World*, Oxford, Hart Publishing, 2010, pp. 1-8.

- Christian Tomuschat, “The International Responsibility of the European Union”, in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *International Law as Law of the European Union*, Leiden, Martinus Nijhoff Publishers, 2012, pp. 177-192.

- Christina Eckes, “International Law as Law of the EU”, in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *International Law as Law of the European Union*, Leiden, Martinus Nijhoff Publishers, 2012, pp. 353-378.

- Christophe Hillion, “Conferral, Cooperation, Balance in EU External Action”, in Marise Cremona, *Structural Principles in EU External Relations Law*, Portland, Hart Publishing, 2018, pp. 117-174.

- Christopher Docksey, “The European Court of Justice and the decade of surveillance”, in Hielke Hijmans and Herke Kranenborg, *Data Protection Anno 2014: How to restore trust? Contributions in Honour of Peter Hustinx, European Data Protection Supervisor 2004-2014*, Uitgevers, Intersentia, 2014, pp. 97-112.

- Christopher Kuner, “Article 44: General Principles for transfer”, in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford, Oxford University Press, 2020, pp. 755-770.

- Christopher Kuner, “Article 45: Transfers on the basis of an adequacy decision”, in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *The EU General Data*

Protection Regulation (GDPR): A Commentary, Oxford, Oxford University Press, 2020, pp. 771-766.

- Christopher Kuner, “Article 50: International cooperation for the protection of personal data”, in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford, Oxford University Press, 2020, pp. 858-859.

- Christopher Kuner, “Developing an Adequate Legal Framework for International Data Transfers”, in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, and Sjaak Nouwt, *Reinventing Data Protection?*, Luxembourg, Springer, 2009, pp. 263-274.

- Claire Potaux, “The Current Role of the International Organization for Migration in developing and implementing Migration and Mobility Partnerships”, in Rahel Kunz, Sandra Lavenex, and Marion Panizzon, *Multilayered migration governance: the promise of partnership*, Abingdon, Routledge, 2011, pp. 183-204.

- Conny Rijken, “Legal and Technical Aspects of Co-operation between Europol, Third States, and Interpol”, in Vincent Kronenberger, *The European Union and the International Legal Order: Discord or Harmony?*, Brussels/Geneva, TMC Asser Press, 2001, pp. 577-603.

- Corien Prins and Wim Voermans, “A Brave New Government?”, in Simone van der Hof and Marga M. Groothuis, *Innovating Government: Normative, Policy and Technological Dimensions of Modern Government*, Springer, The Hague, 2011, pp. 455-466.

- Dag Wiese Schartum, “Sharing Information between Government Agencies: Some Legal Challenges Associated with Semantic Interoperability”, in Simone van der Hof and Marga M. Groothuis, *Innovating Government: Normative, Policy and Technological Dimensions of Modern Government*, The Hague, Springer, 2011, pp. 347-362.

- Dan Svantesson, “Enforcing Privacy Across Different Jurisdictions”, in David Wright and Paul De Hert, *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, Cham, Springer, 2016, pp. 195-222.

- Daniel Warin, “Le rôle du Parlement européen dans le control des agences de l’espace de liberté, sécurité e de justice”, in Cristina Blasi Casagran and Mariona Illamola Dausà, *El control de las agencias del Espacio de Libertad, Seguridad y Justicia*, Madrid, Marcial Pons, 20, pp. 11-20.

- Darrel Ince, “Interoperability”, in Darrel Ince, *A Dictionary of the Internet*, Oxford, Oxford University Press.

- Diana Alonso Blas, “First Pillar and Third Pillar: Need for a Common Approach on Data Protection?”, in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, and Sjaak Nouwt, *Reinventing Data Protection?*, The Netherlands, Springer, 2009, pp. 225-238.

- Dick Heimans, “The External Relations of Europol – Political, Legal and Operational Considerations”, in Bernd Martenczuk and Servaas van Thiel, *Justice, Liberty and Security: New Challenges for EU External Relations*, Brussels, VUB Press, 2008, pp. 385-387.

- Diego Javier Liñán Nogueras “Derechos humanos y libertades fundamentales en la Unión Europea” in Araceli Mangas Martín and Diego Javier Liñán Nogueras, *Instituciones y Derecho de la Unión Europea*, Tecnos, Madrid, 2020, on-line resource.

- Diego Javier Liñán Nogueras, “Derechos Humanos y Unión Europea”, in Jorge Cardona Llorens, *Cursos Euromediterráneos Bancaja Derecho Internacional*, Valencia, Tirant lo Blanch, 2001, pp. 363-440.

- Diego Javier Liñán Nogueras, “La acción de la Unión: las relaciones exteriores (I)”, in Araceli Mangas Martín and Diego Javier Liñán Nogueras, *Instituciones y Derecho de la Unión Europea*, Madrid, Tecnos, 2020, on-line resource.

- Diego Javier Liñán Nogueras, “La acción de la Unión: las relaciones exteriores (II)”, in Araceli Mangas Martín and Diego Javier Liñán Nogueras, *Instituciones y Derecho de la Unión Europea*, Madrid, Tecnos, 2020, on-line resource.

- Diego Javier Liñán Nogueras, “La subjetividad jurídico-internacional de la Unión”, in Araceli Mangas Martín and Diego Javier Liñán Nogueras, *Instituciones y Derecho de la Unión Europea*, Madrid, Tecnos, 2020, on-line resource.

- Diego Javier Liñán Nogueras, “Los derechos fundamentales en la Unión Europea”, in Araceli Mangas Martín and Diego Javier Liñán Nogueras, *Instituciones y Derecho de la Unión Europea*, Madrid, McGraw-Hill, 1996, pp. 581-596.

- Eberhard Schmidt-Aßmann and Fruzsina Molnár-Gábor, “European Administrative Law”, in Anne Peters and Rüdiger Wolfrum, *Max Planck Encyclopedias of International Law*, 2019.

- Edoardo Celeste and Federico Fabbrini, “EU Data Protection Law Between Extraterritoriality and Sovereignty”, in Federico Fabbrini, Edoardo Celeste, and John Quinn, *Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Oxford, Hart Publishing, 2021, pp. 1-15.

- Elaine Fahey, “Transatlantic cooperation in criminal law”, in Valsamis Mitsilegas, Maria Bergström, and Theodore Konstadinides, *Research Handbook on EU Criminal Law*, Cheltenham, Edward Elgar Publishing, 2016, pp. 532-544.

- Eleftheria Neframi, “Customary International Law and Article 3(5) TEU”, in Piet Eeckhout and Manuel Lopez Escudero, *The European Union’s external action in times of crisis*, Oxford, Hart Publishing, 2016, pp. 205-222.

- Eleftheria Neframi, “La répartition des compétences entre l’Union Européenne et ses États Membres en matière d’immigration irrégulière”, in Dubin Laurence, *La légalité de la lutte contre l’immigration irrégulière par l’Union européenne*, Brussels, Bruylant, 2012, pp. 35-63.

- Eleftheria Neframi, “Mixed Agreements as a source of European Union Law”, in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *International Law as Law of the European Union*, Leiden, Martinus Nijhoff Publishers, 2012, pp. 325-352.

- Eleftheria Neframi, “Vertical Division of Competences and the Objectives of the European Union’s External Action”, in Marise Cremona and Anne Thies, *The European Court of Justice and External Relations Law: Constitutional Challenges*, United Kingdom, Hart Publishing, 2014, pp. 73-94.

- Eleni Kosta, “Article 7: Conditions for consent”, in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford, Oxford University Press, 2020, pp. 345-354.

- Ellen Reichel, “Navigating between refugee protection and state sovereignty: legitimating the United Nations High Commissioner for Refugees”, in Laus Dingwerth, Antonia Witt, Ina Lehmann, Ellen Reichel, and Tobias Weise, *International organizations under pressure: legitimating global governance in challenging times*, Oxford, Oxford University Press, 2019, pp. 195-231.

- Ellen Vos, “European Agencies and the Composite Executor”, in Michelle Everson, Cosimo Monda, and Ellen Vos, *European Agencies in between Institutions and Member States*, The Netherlands, Kluwer Law International BV, 2014, pp. 11-47.

- Elspeth Guild, Stefanie Grant and C A Groenendijk, “Unfinished Business: the IOM and Migrants' Human Rights”, in Martin Geiger and Antoine Pécoud, *The International Organization for Migration: the new 'UN Migration Agency' in critical perspective*, Cham, Palgrave Macmillan, 2020, pp. 29-52.

- Enzo Cannizzaro, “The Neo-Monism of the European Legal Order”, in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *International Law as Law of the European Union*, Leiden, Martinus Nijhoff Publishers, 2012, pp. 35-58.

- Esa Paasivirta and Allan Rosas, “Sanctions, Countermeasures and Related Actions in the External Relations of the EU”, in Enzo Cannizzaro, *The European Union as an Actor in International Relations*, The Hague, Kluwer, 2002, pp. 207-218.

- Esa Paasivirta and Thomas Ramopoulos, “UN General Assembly, UN Security Council and UN Human Rights Council”, in Ramses A. Wessel and Jed Odermatt, *Research Handbook on the European Union and International Organizations*, Cheltenham, Edward Elgar Publishing, 2019, pp. 58-81.

- Estanislao Arana García, “The ‘ancillary claim’ for damages in the administrative proceedings”, *Revista Andalucía de Administración Pública*, No. 100, 2018, pp. 25-46.

- Esteve García Francina, “El Control Judicial de las Agencias del Espacio de Libertad, Seguridad y Justicia”, in Cristina Blasi Casagran and Mariona Illamola Dausá, *El control de las agencias del Espacio de Libertad, Seguridad y Justicia*, Madrid, Marcial Pons, 2016, pp. 81-104.

- Federico Casolari, “Giving Indirect Effect to International Law: The Doctrine of Consistent Interpretation”, in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *International Law as Law of the European Union*, Leiden, Martinus Nijhoff Publishers, 2012, pp. 395-416.

- Federico Fabbrini, “The principle of subsidiarity”, in Robert Schutze and Takis Tridimas, *Oxford Principles of European Union law, Vol. I: The European Union Legal Order*, Oxford, Oxford University Press, 2018, pp. 221-242, p. 226.

- Flovi Vlastou-Dimopoulou, “Organisation for Economic Co-operation and Development (OECD)”, in Ramses A. Wessel and Jed Odermatt, *Research Handbook on the European Union and International Organizations*, Cheltenham, Edward Elgar Publishing, 2019, pp. 316-337.

- Francesca Galli, “Interoperable Law Enforcement: Cooperation Challenges in the EU Area of Freedom, Security and Justice”, *EUI Working Papers*, No. 15, 2019, pp. 1-20.

- Francesca Tassinari, “La adopción de actos delegados y actos de ejecución (comentario a los artículos 92 y 93 del RGPD)”, in Antonio Troncoso Reigada, *Comentario al Reglamento general de protección de datos y la ley orgánica de protección de datos personales y garantía de los derechos digitales*, Pamplona, Thomson Reuters Aranzadi, 2021, pp. 4901-4920.

- Francesca Tassinari, “La interoperabilidad de los sistemas de información de gran magnitud de la Unión Europea y la detección de identidades múltiples: garantías y responsabilidades”, in Francisco Javier Garrido Carrillo, *Lucha contra la criminalidad*

organizada y cooperación judicial de la UE: instrumentos, límites y perspectivas en la era digital, Navarra, Thomson Reuters Aranzadi, 2022, pp. 291-338.

- Francesco Salerno, “L'obbligo internazionale di non-refoulement dei richiedenti asilo” in Chiara Favilli, *L'obbligo internazionale di non-refoulement dei richiedenti asilo*, Italy, CEDAM, 2011, pp. 1-33.

- Frank Hoffmeister, “Curse or Blessing? Mixed Agreements in Recent Practice”, in Christophe Hillion and Panos Koutrakos, *Mixed Agreements Revisited: The EU and its Member States in the World*, Oxford, Hart Publishing, 2010, pp. 249-268.

- Fred L Morrison, “Executive Agreements”, in Anne Peters, and Hélène Ruiz Fabri, *Max Planck Encyclopedias of International Law*, New York, Oxford University Press, 2019.

- Gabriela Zafir-Fortuna, “Article 15: Right of access by the data subject”, in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford, Oxford University Press, 2020, pp. 449-468.

- Geert De Baere, “EU external action”, in Catherine Bernard and Steve Peers, *European Union Law*, Oxford, Oxford University Press, 2017, pp. 710-760.

- Geert De Baere, “Subsidiarity as a Structural Principle Governing the use of EU External Competences”, in Marise Cremona, *Structural Principles in EU External Relations Law*, Portland, Hart Publishing, 2018, pp. 71-92.

- Gérard Marcou, “Le thème de l'agence et la réforme des administrations centrales” in Joël Molinier, *Les agences de l'Union européenne*, Brussels, Bruylant, 2011, pp. 3-36.

- Giacomo Gattinara, “Consistent Interpretation of WTO Rulings in the EU Legal Order?”, in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *International Law as Law of the European Union*, Leiden, Martinus Nijhoff Publishers, 2012, pp. 269-290.

- Gianfranco Marullo, “Il ruolo e le attività dei servizi di intelligence e delle forze di polizia nella lotta alla criminalità ed al terrorismo nei paesi dell-Unione Europea, nel rispetto della Convenzione del Consiglio d'Europa sui diritti dell'uomo”, in M. Cherif Bassiouni, *La Cooperazione internazionale per la prevenzione e la repressione della criminalità organizzata e del terrorismo*, Milano, Giuffrè, 2005, pp. 187-208.

- Giorgio Gaja, “Responsabilité des états et/ou des organisations internationales en cas de violations des droits de l'homme: la question de l'attribution”, in Ronny Abraham, *Le droit international des droits de l'homme applicable aux activités des organisations internationales*, Paris, A. Pedone, 2009, pp. 95-103.

- Giulia Tiberi, “Riservatezza e protezione dei dati personali”, in Marta Cartabia, *Il diritto in azione: universalità e pluralismo dei diritti fondamentali nelle Corti europee*, Bologna, Il Mulino, pp. 349-387.

- Gjovalin Macaj and Joachim A. Koops, “Inconvenient multilateralism: The challenges of the EU as a player in the United Nations Human Rights Council”, in Erik Wetzel, *The EU as a “Global Player” in Human Rights*, Oxon, Routledge, 2011, pp. 66-81.

- Gloria González Fuster, “Curtailling a right in flux: restrictions of the right to personal data protection”, in Artemi Rallo Lombarte and Rosario García Mahamut, *Hacia un nuevo derecho europea de protección de datos*, Valencia, Tirant lo Blanch, 2015, pp. 527-528.

- Graham Butles, “United Nations Educational, Scientific and Cultural Organization (UNESCO)”, in Ramses A. Wessel and Jed Odermatt, *Research Handbook on the European Union and International Organizations*, Cheltenham, Edward Elgar Publishing, 2019, pp. 142-164.

- Guy S. Goodwin-Gill, “Non-Refoulement in the 1951 Refugee Convention” in Guy S. Goodwin-Gill, *The refugee in International Law*, Oxford, Clarendon Press, 2007, pp. 201-284.

- Henri Labayle, “The institutional framework”, in Valsamis Mitsilegas, Maria Bergstrom, and Theodore Konstadinides, *Research Handbook on EU Criminal Law*, Cheltenham, Edward Elgar Publishing, 2016, pp. 29-48.

- Herke Kranenborg, “Article 2: Material scope”, in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford, Oxford University Press, 2020, pp. 60-73.

- Herke Kranenborg, “Article 8: Protection of Personal Data”, in Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward, *The EU Charter of Fundamental Rights: A Commentary*, Oregon, Hart Publishing, 2014, pp. 223-266.

- Herwig C.H. Hofmann, “General Principles of EU law and EU administrative law”, in Catherine Barnard and Steve Peers, *European Union Law*, Oxford, Oxford University Press, 2020, pp. 212-242.

- Hielke Hijmans, “Article 1: Subject-matter and objectives”, in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford, Oxford University Press, 2020, pp. 48-59.

- Hielke Hijmans, “Article 51: Supervisory Authority”, in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford, Oxford University Press, 2020, pp. 863-872.

- Ilaria Vianello, “The Rule of Law as a Relationship Principle”, in Marise Cremona, *Structural Principles in EU External Relations Law*, Portland, Hart Publishing, 2020, pp. 225-240.

- Inge Govaere, “Full, Crippled, Split Conferral of Powers Post-Lisbon, in Marise Cremona, *Structural Principles in EU External Relations Law*, Portland, Hart Publishing, 2018, pp. 223-266.

- International Congress of Comparative Law, *Convergence of legal systems in the 21st century: general reports delivered at the XVth Internet*, Brussels, Bruylant, 2006, pp. 1147-1164.

- Jaime Oráa Oraá, “En torno al valor jurídico de la Declaración Universal”, in VV. AA., *La Declaración Universal de Derechos Humanos en su cincuenta aniversario: Un estudio interdisciplinar*, Deusto, Instituto de Derechos Humanos, 1999, pp. 179-202.

- Jaime Oráa Oraá, “The Declaration of Human Rights”, in Felipe Gómez Isa and Koen de Feyter, *International Human Rights Law in a Global Context*, Bilbao, HumanitarianNet, 2009, pp. 163-236.

- Jan Klabbers, “Restraints on the treaty-making powers of Member States deriving from EU Law? Towards a framework for analysis”, in Enzo Cannizzaro, *The European Union as an Actor in International Relations*, The Hague, Kluwer Law International, 2002, pp. 151-176.

- Jan Willem Van Rossem, “The EU at Crossroad: A Constitutional Inquiry into the Way International Law Is Received within the EU Legal Order”, in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *International Law as Law of the European Union*, Leiden, Martinus Nijhoff Publishers, 2012, pp. 59-92.

- Javier Bustamante Donas, “Segundos pensamientos. La cuarta generación de derechos humanos en las redes digitales”, in Paloma Llaneza, *TELOS 85: Los derechos fundamentales en Internet*, Madrid, Fundación Telefónica, 2010, pp. 81-89.

- Jean-Marc Thouvenin, “International Economic Sanctions and Fundamental Rights: Friend or Foe?”, in Norman Weiß and Jean-Marc Thouvenin, *The Influence of Human Rights on International Law*, Cham, Springer, 2015, pp. 113-129.

- Jean-Peter Schneider, “Information exchange and its problems”, in Carol Harlow, Päivi Leino, and Giacinto della Cananea, *Research Handbook on EU Administrative Law*, Cheltenham/Northampton, Edward Elgar Publishing, 2017, pp. 81-112

- Jeanne Pia Mifsud Bonnici, “Redefining the Relationship Between Security, Data Retention and Human Rights”, in Ronald L. Holzhaecker and Paul Luif, *Freedom, Security*

and Justice in the European Union: Internal and External Dimensions of Increased Cooperation after the Lisbon Treaty, New York, Springer, 2014, pp. 49-74.

- Joanne Scott, "The Global Reach of EU Law", in Marise Cremona and Joanne Scott, *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, Oxford, Oxford University Press, 2019, pp. 21-63.

- Joni Helikoski, "The classic authorities revisited", in Alan Dashwood and Joni Hillion, *The General Law of E.C. External Relations*, London, Sweet/Maxwell, 2000, pp. 115-138.

- Joni Heliskoski, "The Arrangement Governing the Relationship between the ECHR and the CJEU in the Draft Treaty on the Accession of the EU to the ECHR", in Marise Cremona and Anne Thies, *The European Court of Justice and External Relations Law: Constitutional Challenges*, United Kingdom, Hart Publishing, 2014, pp. 223-248.

- Jorrit Rijpma, "Hybrid agencification in the Area of Freedom, Security and Justice and its inherent tensions: the case of Frontex", in Madalina Busuioc, Martijn Groenleer, and Jarle Trondal, *The agency phenomenon in the European Union: Emergence, institutionalisation and everyday decision-making*, Manchester, Manchester University Press, 2012, pp. 84-102.

- José Alejandro del Valle, "La fragilidad de los derechos humanos en las fronteras exteriores europeas, y la externalización/extraterritorialidad de los controles migratorios", in Juan Soroeta Liceras and Nicolás Alonso Moreda, *Anuario de los cursos de derechos humanos de Donostia-San Sebastián*, Vol. XVIII, 2019, pp. 25-58.

- José Martín y Pérez de Nanclares, "The protection of human rights in the European Union", in Felipe Gómez Isa and Koen de Feyter, *International Human Rights Law in a Global Context*, Bilbao, HumanitarianNet, 2004, pp. 777-802.

- Josephine Steiner, "Subsidiarity under the Maastricht Treaty", in David O'Keefe and Patrick M. Twomey, *Legal issues of Maastricht Treaty*, Chancery, London, 1994, pp. 49-64.

- Juan Antonio Carrillo Salcedo, "Algunas reflexiones sobre el Valor Jurídico de la Declaración Universal de los Derechos Humanos", in Manuel Pérez González, *Hacia un Nuevo Orden Internacional y Europeo: Homenaje al Profesor Manuel Díez de Velasco*, Madrid, Tecnos, 1993, pp. 167-178.

- Juan Antonio Carrillo Salcedo, "The European Convention on Human rights", in Felipe Gómez Isa and Koen de Feyter, *International Human rights Law in a Global Context*, Deusto, HumanitarianNet, 2009, pp. 631-688.

- Juan Antonio García Jabaloy, "La dimensión exterior de Eurojust: una visión desde la práctica", in Montserrat Pi Llorens and Esther Zapater Duque, *La dimensión exterior de las*

agencias del espacio de libertad, seguridad y justicia, Madrid, Marcial Pons, 2014, pp. 89-100.

- Juan Santos Vara “El acuerdo SWIFT con Estados Unidos: génesis, alcance y consecuencias”, in José Martín y Pérez de Nanclares, *La dimensión exterior del espacio de libertad, seguridad y justicia de la Unión Europea*, Madrid, Iustel, 2012, pp. 355-380.

- Juan Santos Vara and Elaine Fahey, “Transatlantic relations and the operation of AFSJ flexibility”, in Steven Blockmans, *Differentiated integration in the EU from the inside looking out*, Brussels, Centre for European Policy Studies, 2014, pp. 103-126.

- Juan Santos Vara, “Análisis del marco jurídico-político de la dimensión exterior de las agencias del espacio de libertad, seguridad y justicia”, in Montserrat Pi Llorens and Esther Zapater Duque, *La dimensión exterior de las agencias del espacio de libertad, seguridad, y justicia*, Madrid, Marcial Pons Ediciones Jurídicas y Sociales, 2014, pp. 9-34.

- Juan Santos Vara, “Soft international agreements on migration with third countries: a challenge to democratic and judicial controls in the EU”, in Sergio Carrera, Juan Santos Vara, and Tineke Strik, *Constitutionalising the External Dimensions of EU Migration Policies in Times of Crisis: Legality, Rule of Law and Fundamental Rights Reconsidered*, Cheltenham, Edward Elgar Publishing, 2019, pp. 21-38.

- Juan Santos Vara, “The EU’s agencies: Ever more important for the governance of the Area of Freedom, Security and Justice”, in Ariadna Ripoll Servent and Florian Trauner, *The Routledge Handbook of Justice and Home Affairs Research*, United Kingdom, Taylor and Francis Group, 2017, pp. 445-457.

- Julinda Beqiraj, “Strengthening the Cooperation between IOM and the EU in the field of Migration”, in Francesca Ippolito, *Migration in the Mediterranean: mechanisms of international cooperation*, Cambridge, Cambridge University Press, 2015, pp. 115-135.

- Julinda Beqiraj, Jean-Pierre Gauci, and Anna Khalfaoui, “United Nations High Commissioner for Refugees (UNHCR) and International Organization for Migration (IOM)”, in Ramses A. Wessel and Jed Odermatt, *Research Handbook on the European Union and International Organizations*, Cheltenham, Edward Elgar Publishing, 2019, pp. 222-239.

- Kärt Salumaa-Lepik, Tanel Kerikmäe and Nele Nisu, “Data Protection in Estonia”, in Elif Kiesow Cortez, *Data Protection Around the World: Privacy Laws in Action*, The Hague, Springer, 2020, pp. 23-58.

- Katja Lindskov Jacobsen, “New forms of intervention: the case of humanitarian refugee biometrics”, in Nicolas Lemay-Hébert, *Handbook on intervention and statebuilding*, Cheltenham, Edward Elgar Publishing, 2019, pp. 270-281.

- Kevin In-Chuen Koh, “International Organisation for Migration”, in Christian Tietje and Alan Brouder, *Handbook of transnational economic governance regimes*, Leiden, Nijhoff, 2009, pp. 191-200.

- Kieran St C Bradley, “Legislation in the European Union”, in Catherine Barnard and Steve Peers, *European Union Law*, Oxford, Oxford University Press, 2017, pp. 97-142.

- Koen Lenaerts and Amaryllis Verhoeven, “Institutional Balance as a Guarantee for Democracy in EU Governance”, in Christian Joerges and Renaud Dehousse, *Good Governance in Europe’s Integrated Market*, Oxford, Oxford University Press, 2002, pp. 35-88.

- Lee A. Bygrave and Luca Tosoni, “Article 4(7): Controller”, in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford, Oxford University Press, 2020, pp. 145-156.

- Léontin-Jean Constantinesco, “La naturaleza de las Comunidades Europeas”, in Manuel Díez de Velasco Vallejo, *El Derecho de la Comunidad Europea*, Madrid, Universidad Internacional Menéndez Pelayo, 1982, pp. 43-59.

- Loïc Azoulai, “Structural Principles: Internal and External”, in Marise Cremona, *Structural Principles in EU External Relations Law*, Portland, Hart Publishing, 2020, pp. 31-46.

- Ludmila Georgieva, “Article 10: Processing of personal data relating to criminal convictions” in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford, Oxford University Press, 2020, pp. 385-390.

- Luísa Lourenço, “European Economic Area (EEA) and European Free Trade Association (ESTA)”, in Ramses A. Wessel and Jed Odermatt, *Research Handbook on the European Union and International Organizations*, Cheltenham, Edward Elgar Publishing, 2019, pp. 507-528.

- Madeline Garlick, “The Dublin System, Solidarity and Individual Rights”, in Vincent Chetail, Philippe de Bruycker, and Francesco Maiani, *Reforming the Common European Asylum System*, Leiden, Brill Nijhoff, pp. 159-194.

- Marc Maresceau, "A Typology of Mixed Bilateral Agreements", in Christophe Hillion and Panos Koutrakos, *Mixed Agreements Revisited: The EU and its Member States in the World*, Oxford, Hart Publishing, 2010, pp. 55-86.

- Marco Velicogna, "The Making of Pan-European Infrastructure: From the Schengen Information System to the European Arrest Warrant", in Francesco Contini and Giovan Francesco Lanzara, *The Circulation of Agency in E-Justice*, pp. 185-215.

- Marise Cremona "The External Dimension of the Single Market: Building (on) the Foundations", in Catharine Barnard and Joanne Scott, *The Law of the Single European Market: Unpacking the Premises*, London, Hart Publishing, 2002, pp. 351-394.

- Marise Cremona, "A Reticent Court? Policy Objectives and the Court of Justice", in Marise Cremona and Anne Thies, *The European Court of Justice and External Relations Law: Constitutional Challenges*, United Kingdom, Hart Publishing, 2014, pp. 15-32.

- Marise Cremona, "Disconnection Clauses in EU Law and Practices", in Christophe Hillion and Panos Koutrakos, *Mixed Agreements Revisited: The EU and its Member States in the World*, Oxford, Hart Publishing, 2010, pp. 160-186.

- Marise Cremona, "External Relations and External Competence of the European Union: The Emergence of an Integrated Policy", in Paul Craig and Gráinne de Búrca, *The evolution of EU law*, Oxford, Oxford University Press, 2011, pp. 217-268.

- Marise Cremona, "Member States Agreements as Union Law", in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *International Law as Law of the European Union*, Leiden, Martinus Nijhoff Publishers, 2012, pp. 291-324.

- Marise Cremona, "Structural Principles and their Role in EU External Relations Law", in Marise Cremona, *Structural Principles in EU External Relations Law*, Portland, Hart Publishing, 2020, pp. 3-30.

- Marise Cremona, "The External Dimension of the AFSJ", in Marise Cremona, Jörg Monar and Sara Poli, *The External Dimension of the European Union's Area of Freedom, Security, and Justice*, Brussels, College of Europe Studies, 2010, pp. 77-118.

- Marjorie Beaulay, "Human Rights Protection and the Notion of Responsibility: Some Considerations About the European Case Law on State's Activities under U.N. Charter", in Norman WeißJean and Marc Thouvenin, *The Influence of Human Rights on International Law*, Cham, Springer, 2015, pp. 93-110.

- Marton Varju, "European human rights law as a multi-layered human rights regime. Preserving diversity and promoting human rights", in Erik Wetzel, *The EU as a "Global Player" in Human Rights?*, Oxon, Routledge, 2011, pp. 49-65.

- Mathias Forteau, “Le droit applicable en matière de droits de l’homme aux administrations territoriales gérées par des organisations internationales”, in Ronny Abraham, *Le droit international des droits de l’homme applicable aux activités des organisations internationales*, Paris, A. Pedone, 2009, pp. 7-34.

- Mauro Gatti, “Conflict of Legal Basis and the Internal–External Security Nexus: AFSJ versus CFS”, in Eleftheria Neframi and Mauro Gatti, *Constitutional Issues of EU External Relations Law*, Baden-Baden, Nomos, 2018, pp. 89-110.

- Merijn Chamon, “Provisional Application’s Novel Rationale: Facilitating Mixity in the EU’s Treaty Practice”, in Wybe Th. Douma, *The Evolving Nature of EU External Relations Law*, Berlin-Heidelberg, Springer, 2021, pp. 131-163.

- Michelle Everson, “European Agencies: Barely Legal?”, in Michelle Everson, Cosimo Monda, and Ellen Vos, *European Agencies in between Institutions and Member States*, The Netherlands, Kluwer Law International BV, 2014, pp. 49-70.

- Mirentxu Jordana Santiago, “La dimensión exterior de Eurojust: medios de actuación y mecanismos de control”, in Montserrat Pi Llorens and Esther Zapater Duque, *La dimensión exterior de las agencias del espacio de libertad, seguridad y justicia*, Madrid, Marcial Pons, 2014, pp. 69-88.

- Niels Petersen, "The Role of Consent and Uncertainty in the Formation of Customary International Law", in Brian D. Lepard, *Reexamining Customary International Law*, Cambridge, Cambridge University Press, pp. 111-130.

- Niovi Vavoula, “Interoperability of EU Information Systems in a ‘Panopticon’ Union: A Leap Towards Maximised Use of Third-Country Nationals’ Data or Step Backwards in the Protection of Fundamental Rights?”, in Valsamis Mitsilegas and Niovi Vavoula, *Surveillance and Privacy in the Digital Age: European Transatlantic and Global Perspectives*, London, Hart Publishing, 2021, pp. 159-195.

- Pablo Jesús Martín Rodríguez, “Confianza mutua y derechos fundamentales en el espacio de libertad, seguridad y justicia”, in Alejandro Sánchez Frías, Francisco Peña Díaz, Ana Salinas de Frías, and Enrique J. Martínez Pérez, *La Unión Europea y la protección de los derechos fundamentales*, 2018, pp. 247-258.

- Pablo Jesús Martín Rodríguez, “La insoportable levedad de la confianza mutua en el espacio de libertad, seguridad y justicia”, in José Manuel Cortés Martín and Florentino-Gregorio Ruiz Yamuza, *Retos actuales de la cooperación penal en la Unión Europea*, 2020, pp. 95-124.

- Paolo Palchetti, "Judicial Review of the International Validity of UN Security Council Resolutions by the European Court of Justice", in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *International Law as Law of the European Union*, Leiden, Martinus Nijhoff Publishers, 2012, pp. 379-394.

- Paolo Palchetti, "Reactions by the European Union to breaches of Erga Omnes Obligations", in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *International Law as Law of the European Union*, Leiden, Martinus Nijhoff Publishers, 2012, pp. 379-394.

- Patrick Grother, "Interoperable Performance", in Li Stan Z., Jain Anil K., *Encyclopedia of Biometrics*, New York, Springer, 2015, pp. 941-946.

- Paul De Hert and Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action", in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, and Sjaak Nouwt, *Reinventing Data Protection?*, Dordrecht, Springer, 2009, pp. 3-44.

- Paul De Hert and Vagelis Papakonstantinou, "Data protection policies in EU justice and home affairs: A multi-layered and yet unexplored territory for legal research", in Aradna Ripoll Servent and Florian Trauner, *The Routledge Handbook of Justice and Home Affairs research*, United Kingdom, Taylor and Francis Group, 2017, pp. 169-179.

- Paul De Hert, "EU criminal law and fundamental rights", in Valsamis Mitsilegas, Maria Bergström, and Theodore Konstadinides, *Research Handbook on EU Criminal Law*, Elgar Edward Publishing, 2016, pp. 105-124.

- Paul De Hert, "EU Sanctioning Powers and Data Protection: New Tools for Ensuring the Effectiveness of the GDPR in the Spirit of Cooperative Federalism", in Stefano Montaldo, Francesco Costamagna, and Alberto Miglio, *EU Law Enforcement: The Evolution of Sanctioning Powers*, Oxford, Routledge, 2021, pp. 291-324.

- Paul Trattuttmansdoff, "The Politics of Digital Borders", in Cengiz Günay and Nina Witjes, *Border Politics*, Cham, Springer International Publishing, 2017, pp. 107-126.

- Paula García Andrade, "La geometría variable y la dimensión exterior del ELSJ", in José Martín y Pérez de Nanclares, *La dimensión Exterior del Espacio de Libertad, Seguridad y Justicia en la Unión Europea*, Madrid, Iustel, 2012, pp. 87-124.

- Paz Andrés Sáenz de Santa María, "El Estado de derecho en el sistema institucional de la Unión europea: Realidades y desafíos", in Diego Javier Liñán Noguerras and Pablo Jesús Martín Rodríguez, *Estado de Derecho y Unión Europea*, Madrid, Tecnos, 2018, pp. 129-156.

- Peter Hustinx, "EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation", in Marise Cremona, *New Technologies and EU Law*, Oxford, Oxford University Press, 2017, pp. 123-173.

- Petr Dostál, "Changing European Union: The Schengen Agreement", in Tomáš Havlíček, Milan Jeřábek, and Jaroslav Dokoupil, *Borders in Central Europe After the Schengen Agreement*, Cham, Springer, 2017, pp. 15-35.

- Piet Eeckhout, "The Integration of Public International Law in EU Law: Analytical and Normative Questions", in Piet Eeckhout and Manuel Lopez Escudero, *The European Union's external action in times of crisis*, Oxford, Hart Publishing, 2016, pp. 189-204.

- Pieter Jan Kuijper, "Case Law of the Court of Justice of the EU and the Allocation of External Relation Powers", in Marise Cremona and Anne Thies, *The European Court of Justice and external relations law: Constitutional Challenges*, Oxford, Hart Publishing, 2013, pp. 95-114.

- Pika Šarf, "Automating Freedom, Security and Justice: Interoperability of AFSJ Databases as a Move Towards the Indiscriminate Mass Surveillance of Third-Country Nationals", in Aleš Završnik and Vasja Badalič, *Automating Crime Prevention, Surveillance, and Military Operations*, Switzerland, Springer, 2021, pp. 85-108.

- R. Daniel Kelemen, "European Union Agencies", in Erik Jones, Anand Menon, and Stephen Weatherill, *The Oxford Handbook of the European Union*, Oxford, Oxford University Press, 2014, pp. 392-406.

- Rajeev Gupta, Himanshu Gupta, and Mukesh Mohania, "Cloud Computing and Big Data Analytics: What Is New from Databases Perspective?", in Srinath Srinivasa and Vasudha Bhatnagar, *Big Data Analytics: Lecture Notes in Computer Science*, Berlin/Heidelberg, Springer, 2012, pp. 42-61.

- Ramses A Wessel, "Cross-pillar Mixity", in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *International Law as Law of the European Union*, Leiden, Martinus Nijhoff Publishers, 2012, pp. 30-54.

- Ramses A. Wessel, "Relationship Between International and EU Law", in Enzo Cannizzaro, Paolo Palchetti, and Ramses A. Wessel, *International Law as Law of the European Union*, Leiden, Martinus Nijhoff Publishers, 2012, pp. 7-34.

- Ramses A. Wessel, Luisa Marin, and Claudio Matera, "The External Dimension of the EU's Area of Freedom, Security and Justice", in Christina Eckes and Theodore Konstadinides, *Crime within the Area of Freedom, Security and Justice: A European Public Order*, Cambridge, Cambridge University Press 2011, pp. 272-300.

- Renaud Dehousse, “Misfits: EU Law and the Transformation of European Governance”, in Christian Joerges and Renaud Dehousse, *Good Governance in Europe’s Integrated Market*, Oxford, Oxford University Press, 2002, pp. 207-216.
- Richard B. Lillich, “Duties of States Regarding the Civil Rights of Aliens”, *Collected Courses of the Hague Academy of International Law*, Vol. 161, 1978, pp. 329-442.
- Robert Schütze, “Classifying EU competences: German Constitutional Lesson?”, in Sacha Garben and Inge Govaere, *The division of competences between the EU and the member States*, Oxford, Hart Publishing, 2017, pp. 33-58.
- Robert Schütze, “Federalism and Foreign Affairs: Mixity as an (Inter)national Phenomenon”, in Christophe Hillion and Panos Koutrakos, *Mixed Agreements Revisited: The EU and its Member States in the World*, Oxford, Hart Publishing, 2010, pp. 55-86.
- Rosaria Sicurella, “EU competence in criminal matters”, Valsamis Mitsilegas, Maria Bergstrom, and Theodore Konstadinides, *Research Handbook on EU Criminal Law*, Cheltenham, Edward Elgar Publishing, 2016, pp. 49-77.
- Serena Forlati, “Il Parere 2/13 Della Corte Di Giustizia Dell’Unione Europea: Quale Avvenire Per Lo Spazio Di Libertà, Sicurezza e Giustizia e Per La Tutela Multilivello Dei Diritti Fondamentali In Europa?”, in VV. AA., *Globalización, Derecho y Cambios Sociales*, Santa Fe Argentina, Universidad Nacional del Litoral, 2017, pp. 205-231.
- Sionaidh Douglas-Scott, “The European Union Fundamental Rights”, in Robert Schütze and Takis Tridimas, *Oxford Principles of European Union law, Vol. I: The European Union Legal Order*, Oxford, Oxford University Press, 2018, pp. 383-422.
- Sobrino Heredia and Rey Aneiros, “Las relaciones entre los Estados Partes en un tratado celebrado por una Organización Internacional y los Estados miembros de ésta”, in Mariño Menéndez, *El Derecho Internacional en los albores del siglo XXI: Homenaje al Profesor Juan Manuel Castro-Rial Canosa*, Madrid, Trotta, 2002, pp. 559-638.
- Sobrino Heredia, “La subjetividad internacional de las organizaciones internacionales”, in Manuel Díez de Velasco, *Instituciones de Derecho Internacional Público*, Madrid, Tecnos, 2016, pp. 346-370.
- Stefano Saluzzo, “The EU as a Global Standard Setting Actor: The Case of Data Transfers to Third Countries”, in Elena Carpanelli and Nicole Lazzarini, *Use and Misuse of New Technologies: Contemporary Challenges in International and European Law*, Switzerland, Springer, 2019, pp. 115-134.

- Stephen Weatherill, "Beyond Preemption? Shared Competence and Constitutional Change in the European Community", in David O'Keefe and Patrick M. Twomey, *Legal issues of Maastricht Treaty*, London, Chancery, 1994, pp. 227-230.

- Steve Peers, "EU Justice and Home Affairs Law (Non-Civil)", in Paul Craig and Gráinne de Búrca, *The Evolution of EU Law*, Oxford, Oxford University Press, 2011, pp. 272-274.

- T. Alexander Aleinikoff, "The Mandate of the Office of the United Nations High Commissioner for Refugees", in Vincent Chetail and Céline Bauloz, *Research handbook on international law and migration*, UK/US, Edward Elgar Publishing, 2014, pp. 389-416.

- Takis Tridimas, "The principle of proportionality", in Robert Schütze and Takis Tridimas, *Oxford Principles of European Union law, Vol. I: The European Union Legal Order*, Oxford, Oxford University Press, 2018, pp., 221-242, p. 247.

- Torben Holvad, "Mutual recognition, standards and interoperability", in Matthias Finger and Pierre Messulam, *Rail economics, regulation and policy in Europe*, Cheltenham, Edward Elgar Publishing, 2015, pp. 275-302.

- Violeta Moreno-Lax and Cathryn Costello, "The Extraterritorial Application of the EU Charter of the Fundamental Rights? From Territoriality to Facticity, the Effectiveness Model", in Steve Peers, Tamara K Hervey, Jeff Kenner, and Angela Ward, *The EU Charter of Fundamental Rights: A Commentary*, Oxford, Hart Publishing, 2014, pp. 1700-1727.

- Waltraut Kotschy, "Article 6: Lawfulness of processing", in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A commentary*, Oxford, Oxford University Press, pp. 321-344.

Journal contribution

- A. Cançado Trindade, "Mechanisms of International Protection", *Collected Courses of the Hague Academy of International Law*, Vol. 202, 1987, pp. 9-435.

- Agnes Hurwitz, "The 1990 Dublin Convention: A Comprehensive Assessment", *International Journal of Refugee Law*, Vol. 11, 1999, pp. 646-677.

- Alexander Zinser, "European Data Protection Directive: The Determination of the Adequacy Requirement in International Data Transfers", *Tulane Journal of Technology and Intellectual Property*, No. 6, 2004, pp. 171-180.

- Alexander Zinser, "International Data Transfer out of the European Union: The Adequate Level of Data Protection According to Article 25 of the European Data Protection Directive", *John Marshall Journal of Computer and Information Law*, Vol. 21, No. 4, 2003, pp. 547-566.

- Alison White, "Control of Transborder Data Flow: Reactions to the European Data Protection Directive", *International Journal of Law and Information Technology*, Vol. 5, No. 2, 1997, pp. 230-247.
- Álvaro Oliveira, "Case C-170/96, Commission of the European Communities v. Council of the European Union, judgment of 12 May 1998, [1998] ECR I-2763", *Common Market Law Review*, Vol. 36, No. 1, 1999, pp. 149-155.
- Amedeo Santusuosso and Alessandra Malerba, "Legal Interoperability as a Comprehensive Concept in Transnational Law", *Law, Innovation and Technology*, Vol. 6 No. 51, 2014, pp. 51-73.
- Ana Gascon Marcén, "The extraterritorial application of European Union Data Protection Law", *Spanish Yearbook of International Law*, No. 233, 2019, pp. 413-425.
- Andrea Blasi, "La protezione dei dati personali nella Giurisprudenza della Corte europea dei diritti dell'uomo", *Rivista internazionale dei diritti dell'uomo*, Vol. 12, No. 2, 1999, pp. 543-559.
- Andrea Ott, "EU regulatory agencies in EU external relations: Trapped in a legal minefield between European and international law", *European Foreign Affairs Review*, Vol. 13, No. 4, 2008, pp. 515-540.
- Andrea Ott, Ellen Vos, and Florin Coman-Kund, "EU agencies and their international mandate: A new category of global actors?", *Centre for the law of the EU external relations Working Paper*, No. 7, 2013, pp. 1-38.
- Andrew Clapham, "Human Rights in Armed Conflict: Metaphors, Maxims, and the Move to Interoperability", *Human Rights & International Legal Discourse*, Vol. 12, No. 1, 2018, pp. 9-22.
- Andrew D Selbst and Julia Powles, "Meaningful information and the right to explanation", *International Data Privacy Law*, Vol. 7, No. 4, 2017, pp. 233-242.
- Anja Møller Pedersen, Henrik Udsen, and Søren Sandfeld Jakobsen, "Data retention in Europe—the Tele 2 case and beyond", *International Data Privacy Law*, 2018, Vol. 8, No. 2, pp. 160-174.
- Anna Lodinová, "Application of biometrics as a means of refugee registration: focusing on UNHCR's strategy", *Development, Environment and Foresight*, Vol. 2, No. 2, 2016, pp. 91-100.
- Anna Zharova, "Influence of the Principle of Interoperability on Legal Regulation", *International Journal of Law and Management*, Vol. 57, No. 6, 2015, pp. 562-572.

- Antonella Galletta and Paul De Hert, "The proceduralisation of Data protest Remedies under EU Data Protection Law: Towards a More Effective and Data Remedial System?", *Review of European Administrative Law*, Vol. 8, No. 1, 2015, pp. 125-151.
- Antonio Segura Serrano, "Ciberseguridad y Derecho internacional", *Revista española de derecho internacional*, Vol. 69, No. 2, 2017, pp. 291-299.
- Antonio-Enrique Pérez Luño, "Las Generaciones de Derechos Humanos", *Revista de Centro de Estudios Constitucionales*, No. 10, 1991, pp. 203-217.
- Arianna Vidaschi, "Privacy and data protection versus national security in transnational flights: the EU–Canada PNR agreement", *International Data Privacy Law*, 2018, Vol. 8, No. 2, pp. 124-139.
- Ben Hayes, "Migration and Data Protection: Doing No Harm in an Age of Mass Displacement, Mass Surveillance and Big Data", *International Review of the Red Cross*, Vol. 99, No. 179, 2017, pp. 179-210.
- Benjamin Greze, "The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives", *International Data Privacy Law*, No. 2, Vol. 9, 2019, pp. 109-128.
- Bernhard Maier, "How Has the Law Attempted to Tackle the Borderless Nature of the Internet?", *International Journal of Law and Information Technology*, No. 2, Vol. 18, 2010, pp. 142-175.
- Beth A. Simmons, "Compliance with international agreements", *Annual Review Political Science*, No. 1, 1998, pp. 75-93.
- Bruno Simma and Philip Alston, "The sources of human rights law: custom, jus cogens, and general principles", *Australian Yearbook of International Law*, pp. 82-108.
- Bryce Goodman and Seth Flaxman, "European Union regulations on algorithmic decision-making and a 'right to an explanation'", *ICML Workshop on Human Interpretability in Machine Learning* (WHI 2016), 2016, pp. 1-9.
- Carly Nyst and Tomaso Falchetta, "The Right to Privacy in the Digital Age", *Journal of Human Rights Practice*, No. 9, 2017, pp. 104-118.
- Cathal Flynn, "Data Retention, the Separation of Power in the EU and the Right to Privacy: A Critical Analysis of the Legal Validity of the 2006 Directive on the Retention of Data", *University College Dublin Law Review*, No. 8, 2008, pp. 1-24.
- Catherine Phoung, "The Dublin Convention on Asylum: Its Essence, Implementation and Prospects", *European Public Law*, Vol. 7, 2001, pp. 325-327.

- Cedric Ryngaert and Mistale Taylor, "The GDPR as Global Data Protection Regulation?", *American Journal of International Law Unbound*, Vol. 114, 2020 pp. 5-9.
- César Nava Escudero, "El acuerdo de París. Predominio del soft law en el régimen climático", *Boletín Mexicano de Derecho Comparado*, No. 147, Vol. 49, 2016, pp. 99-135.
- Charlotte Bagger Tranberg, "Proportionality and data protection in the case law of the European Court of Justice", *International Data Privacy Law*, Vol. 1, No. 4, 2011, pp. 239-248.
- Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen Borgesius, "The European Union general data protection regulation: what it is and what it means", *Information & Communications Technology Law*, Vol. 28, No. 1, 2019, p. 65-98.
- Christine M. Chinkin, "United Nations Accountability for Violations of International Human Rights Law", *The Hague Academy of International Law*, Vol. 395, 2018, pp. 199-320.
- Christopher Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 2)", *International Journal of Law and Information Technology*, No. 3, Vol. 18, 2010, pp. 227-247.
- Christopher Kuner, "Extraterritoriality and international data transfers in EU law", *International Data Privacy Law*, No. 4, Vol. 5, 2015, pp. 235-245.
- Christopher Kuner, "International Organizations and the EU General Data Protection Regulation", *International Organization Law Review*, No. 16, 2019, pp. 158-191.
- Christopher Kuner, "Reality and Illusion in EU Data Transfer Regulation Post Schrems", in *German Law Journal*, 2017, pp. 881-918.
- Christopher Kuner, Fred H. Cate, Christopher Millard, and Dan Jerker B. Svantesson, "PRISM and privacy: Will this change everything?", *International Data Privacy Law*, Vol. 3, No. 4, 2013, pp. 217-219,
- Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson, "The extraterritoriality of data privacy laws—an explosive issue yet to detonate", *International Data Privacy Law*, No. 3, Vol. 3, 2013, pp. 147-148.
- Cinzia Peraro, "Protezione extraterritoriale dei diritti: il trasferimento dei dati personali dall'Unione Europea verso paesi terzi", *Rivista Ordine Internazionale e Diritti Umani*, No. 3, 2021, pp. 666-691.
- Clare Sullivan, "EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era", *Computer Law & Security Review*, No. 35, 2019, pp. 380-397.

- Colonel Kirby Abbott, "A brief overview of legal interoperability challenges for NATO arising from the interrelationship between IHL and IHRL in light of the European Convention on Human Rights", *International Review of the Red Cross*, No. 96, Vol. 893, 2014, pp. 107-137.

- Concepción Escobar Hernández, "El convenio de aplicación de Schengen y el Convenio de Dublín: una aproximación al asilo desde la perspectiva comunitaria", *Revista de instituciones europeas*, 1993, pp. 53-100.

- Dan Jerker B Svantesson, "A "layered approach" to the extraterritoriality of data privacy laws", *International Data Privacy Law*, No. 3, Vol. 4, 2013, pp. 278-286.

- Dan Jerker B Svantesson, "Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation", *International Data Privacy Law*, No. 4, Vol. 5, 2015, pp. 226-234.

- Dan Jerker B Svantesson, "The regulation of cross-border data flows", *International Data Privacy Law*, No. 1, Vol. 3, 2011, pp. 180-198.

- Dan Svantesson, "Fundamental Policy Considerations for the Regulation of Internet Cross- border Privacy Issues", *Policy and Internet*, Vol. 3, No. 3, 2011, pp. 1-22.

- Daniel Bodansky, "Legally binding versus non- legally binding instruments", in Scott Barrett Carlo Carraro, and Jaime de Melo, *Towards a Workable and Effective Climate Regime*, London /France, CEPR Press/Ferdi, 2015, pp. 155-165.

- Daniel Drewer and Vesela Miladinova, "The BIG DATA Challenge: Impact and Opportunity of Large Quantities of Information Under the Europol Regulation", *Computer Law & Security Review*, Vol. 33, No. 3, 2017, pp. 298-308.

- Daniel T. Murphy, "The Restatement (Third)'s Human Rights Provisions: Nothing New, But Very Welcome", *The International Lawyer*, No. 24, 1990, pp. 917-930.

- Dariusz Adamski, "The European Securities and Markets Authority Doctrine: A Constitutional Revolution and Economics of Delegation", *European Law Review*, Vol. 6, No. 39, pp. 812-834.

- David Fernández Rojo, "El diseño de una administración supranacional e integrada para el espacio europeo de libertad, seguridad y justicia", *Revista General de Derecho Administrativo*, No. 58, 2021, pp. 1-40.

- David O'Keeffe, "The Schengen Convention: A Suitable Model for European Integration?", *Yearbook of European Law*, Vol. 1, No. 11, 1991, pp. 185-219.

- Davor Jančić, “The Role of the European Parliament and the US Congress in Shaping Transatlantic Relations: TTIP, NSA Surveillance, and CIA Renditions”, *Journal Common Market Studies*, Vol. 54, No. 4, 2016, pp. 896-912.
- Deirdre Curtin and Filipe Brito Bastos, “Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue”, *European Public Law*, Vol. 26, No. 1, 2020, pp. 59-70.
- Didier Bigo, Lina Ewert, and Elif Mendos Kuşkonmaz, “The interoperability controversy or how to fail successfully: lessons from Europe”, *Int. J. Migration and Border Studies*, Vol. 6, Nos. 1/2, 2020, pp. 93-114.
- Editor’s Note, “Discussions: What are the future challenges for humanitarian action?”, *International Review of the Red Cross*, Vol. 93, No. 884, 2011, pp. 899-914.
- Elaine Fahey, “Swimming in a sea of law: Reflections on water borders, Irish(-British)-Euro Relations and opting-out and opting-in after the Treaty of Lisbon”, *Common Market Law Review*, Vol. 47, No. 3, 2010, pp. 673-707.
- Eliantonio Mariolina, “Information Exchange in European Administrative Law. A Threat to Effective Judicial Protection?”, *Maastricht Journal of European and Comparative Law*, No. 3, 2016, pp. 531-549.
- Elisabeth Hoffberger-Pippan, “The Interoperability of EU Information Systems and Fundamental Rights concerns”, *Spanish Yearbook of International Law*, No. 23, 2019, pp. 426-250.
- Elise Muir, “Fundamental Rights: An Unsettling EU Competence”, *Human Rights Review*, 2014, Vol. 15, pp. 25–37.
- Ellen Vos, “Reforming the European Commission: what role to play for EU agencies?”, *Common Market Law Review*, Vol. 37, 2000, pp. 1113-1134.
- Elspeth Guild, “The UN's Search for a Global Compact on Safe, Orderly and Regular Migration”, *German law journal: review of developments in German, European and international jurisprudence*, Vol. 18, No. 7, 2017, pp. 1779-1795.
- Emilio De Capitani, “The Schengen system after Lisbon: from cooperation to integration”, *ERA Forum*, No. 15, 2014, pp. 101-118.
- Enrico Massa, “L'evoluzione del diritto internazionale dei rifugiati attraverso la partecipazione dell'ACNUR alla funzione giurisdizionale”, *La Comunità Internazionale: rivista trimestrale della Società Italiana per l'Organizzazione Internazionale*, Vol. 74, No. 3, 2019, pp. 419-445.

- Evelien Brouwer, "Large-Scale Databases and Interoperability in Migration and Border Policies: The Non- Discriminatory Approach of Data Protection", *European Public Law*, Vol. 26, No. 1, 2020, pp. 71-92.

- Felix Ermacora, "Human Rights and Domestic Jurisdiction", *Collected Courses of The Hague Academy of International Law*, Vol. 124, 1968, pp. 371-452.

- Florian Aumond, "Responsabilité des organisations internationales et droits fondamentaux. L'exemple de l'ONU dans le contexte de l'administration et de la gestion des camps de réfugiés et de déplacés internes par le HCR", *Les responsabilités*, 2018, pp. 5-24.

- Florin Coman-Kund, "EU agencies as global actors: a legal assessment of Europol's international dimension", *Maastricht Faculty of Law Working Paper*, No. 6, 2014, pp. 1-43.

- Florin Coman-Kund, "Europol's International Exchanges of Data and Interoperability of AFSJ Databases", *European Public Law*, Vol. 26, No. 1, 2020, pp. 181-204.

- Florin Coman-Kund, "The International Dimension of the EU Agencies: Framing a Framing Legal-Institutional Phenomenon", *European Foreign Affairs Review*, Vol. 23, No. 1, 2018, pp. 97-118.

- Francesca Tassinari, "La transmisión de información fiscal frente a la Carta de Derechos Fundamentales: reflexiones sobre la Sentencia del Tribunal de Justicia de 6 de octubre de 2020, État Luxembourgeois", *Revista de Derecho Comunitario Europeo*, No. 69, 2021, pp. 683-703.

- Francesca Tassinari, "The externalisation of Europe's data protection law in Morocco: an imperative means for the management of migration flows", *Peace & Security - Paix et Sécurité Internationales (Euro Mediterranean Journal of International Law and International Relations)*, No. 9, 2021, pp. 1-24.

- Francesca Tassinari, "The European Union Adequacy Standard in the Field of Data Protection: A Competence Approach", *Diritti Umani e Diritto Internazionale*, No. 1, Vol. 16, 2022, pp. 5-38.

- Francesco Salerno, "L'obbligo internazionale di non-refoulement dei richiedenti asilo", *Diritti umani e diritto internazionale*, No. 3, 2010, pp. 487-515.

- Francis Aldhouse, "The Transfer of Personal Data to Third Countries Under EU Directive 95/46/EC", *International Review of Law Computers & Technology*, No. 1, Vol. 13, 1999, pp. 75-79.

- François Lafarge, "Administrative Cooperation between Member States and Implementation of EU Law", *European Public Law*, No. 4, Vol. 16, 2010, pp. 597-616.

- Fulvio Attino, "EU's Humanitarian and Civil Protection Aid: Italy's Eccentric and ECHO-Consistent Policy", *Romanian Journal of European Affairs*, Vol. 16, No. 24, 2016, pp. 24-43.

- Gabe Maldoff and Omer Tene, "Essential Equivalence and European Adequacy after Schrems: The Canadian Example", *Wisconsin International Law Journal*, Vol. 34, 2016, pp. 211-283.

- Gianclaudio Malgieri and Giovanni Comand , "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", *International Data Privacy Law*, Vol. 7, No. 4, 2017, pp. 243-265.

- Giandomenico Majone, "Delegation of Regulatory Powers in a Mixed Polity", *European Law Journal*, Vol. 8, No. 3, 2002, pp. 319-339.

- Gianpaolo Maria Ruotolo, "Hey! You! Get OV My Cloud! Accesso autoritativo alle nuvole informatiche e diritto internazionale", *Archivio Penale*, No. 3, 2013, pp. 853-864.

- Giovanni Barontini, "Sulla competenza per l'esame delle domande di asilo secondo le convenzioni di Schengen e Dublino", *Rivista di Diritto Internazionale*, Vol. 75, No. 2, 1992, pp. 335-347.

- Gloria Gonz lez Fuster and Serge Gutwirth, "Opening up personal data protection: a conceptual controversy", *Computer Law & Security Review*, No. 29, 2013, pp. 531-539.

- Goran Bandov and Gabrijela Gosovic, "Humanitarian Aid Policies within the European Union External Action", *Journal of Liberty and International Affairs*, Vol. 4, No. 2, 2018, pp. 25-39.

- Graham Pearce and Nicholas Platten, "Achieving Personal Data Protection in the European Union", *Journal of Common Market Studies*, No. 36, 1998, pp. 529-548.

- Greenleaf, Graham, "Data Protection Convention 108 Accession Eligibility: 80 Parties Now Possible (August 31, 2017)", *Privacy Laws & Business International Report*, No. 148, 2018, pp. 12-16.

- Greer Damon, "Safe harbor—a framework that works", *International Data Privacy Law*, No. 1, Vol. 3, 2011, pp. 143-148.

- Gregor Schusterschitz, "European Agencies as Subjects of International Law", *International Organizations Law Review*, Vol. 1, 2004, pp. 163-188.

- Guy S. Goodwin-Gill, "The Office of the United States High Commissioner for Refugees and the Sources of international Refugee Law", *International and comparative law quarterly*, Vol. 69, No. 1, 2020, pp. 1-41.

- H. Franken and A. K. Koekkoek, "The protection of fundamental rights in a digital age", in VV. AA., *Convergence of legal systems in the 21st century: general reports delivered at the XVIth International Congress of Comparative Law (Brisbane, Australia, 14-20 July 2002)*, Brussels, Bruylant, 2006, pp. 1147-1164.

- Hartmut Aden, "Interoperability Between EU Policing and Migration Databases: Risks for Privacy", *European Public Law*, Vol. 26, No. 1, 2020, pp. 93-108.

- Helena Torroja Mateu, "La «protección diplomática» de los «derechos humanos» de los nacionales en el extranjero: ¿situaciones jurídicas subjetivas en tensión?", *Revista Española de Derecho Internacional*, Vol. 58, No. 1, 2006, pp. 215-237.

- Hersch Lauterpacht, "The International Protection of Human Rights", *Collected Courses of the Academy of International Law*, Vol. 70, 1947, pp. 5-105.

- Hielke Hijmans and Alfonso Scirocco, "Shortcomings in EU data protection in the third and the second pillars. Can the Lisbon treaty be expected to help?", *Common Market Law Review*, No. 46, 2009, pp. 1485-1525.

- Horst Günter Krenzle and Christian Pitschas, "Progress or Stagnation? The Common Commercial Policy After Nice", *European Finance Review*, No. 6, 2001, pp. 308-309.

- Ioanna Tourkochuriti, "The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide between U.S.-EU in Data Privacy Protection", *University of Arkansas at Little Rock Law Review*, Vol. 36, No. 2, 2014, pp. 161-176.

- Itziar Sobrino García, "Las decisiones de adecuación en las transferencias internacionales de datos. el caso del flujo de datos entre la Unión Europea y Estados Unidos", *Revista de Derecho Comunitario Europeo*, No. 68, 2021, pp. 227-256.

- J. A. Winter, "Direct Applicability and Direct Effect", *Common Market Law Review*, Vol. 9, 1972, pp. 425-438.

- Jana Puglierin, "Priorities for the EU's New Foreign Policy Agenda up to 2024: Unleashing the Potential of the Common Foreign and Security Policy", *DGAP Analysis*, No. 1, 2019.

- Jason Coppel and Aidan O' Neill, "The European Court of Justice: taking rights seriously", *Common Market Law Review*, Vol. 29, No. 4, 1992, pp. 669-692.

- Jennifer Cobbe, "Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making", *Legal Studies*, Vol. 39, No. 4, 2019, pp. 636-655.

- John R. Den, “Maintaining transatlantic strategic, operational and tactical interoperability in an era of austerity”, *International Affairs (Royal Institute of International Affairs 1944-)*, Vol. 90, No. 3, 2014, pp. 583-600.

- Jörg Hoffmann and Begoña Gonzalez Otero, “Demystifying the Role of Data Interoperability in the Access and Sharing Debate”, *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, Vol. 11, No. 3, 2020, pp. 252-273.

- Jörg Polakiewicz, “A Council of Europe perspective on the European Union: Crucial and complex cooperation”, *Europe and the World: A law review*, Vol. 5, No. 1, 2021, pp. 1-19.

- Jorrit Rijpma, “Case C-77/05, United Kingdom v. Council, Judgment of the Grand Chamber of 18 December 2007, not yet reported, and Case C-137/05, United Kingdom v. Council, Judgment of the Grand Chamber of 18 December 2007, not yet reported”, *Common Market Law Review*, Vol. 45, No. 3, 2008, pp. 835-852.

- Jos Dumortier, “The Protection of Personal data in the Schengen Convention”, *International Review of Law Computers and Technology*, Vol. 11, No. 1, 1997, pp. 93-106.

- José Alejandro del Valle Gálvez, “Control de Fronteras y Unión Europea”, *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid*, No. 7, 2003, pp. 67-92.

- José Alejandro del Valle, “Inmigración, derechos humanos y modelo europeo de fronteras. Propuestas conceptuales sobre ‘extraterritorialidad’, ‘desterritorialidad’ y ‘externalización’ de controles y flujos migratorios”, *Revista de Estudios Jurídicos y Criminológicos*, No. 2, Universidad de Cádiz, 2020, pp. 145-210.

- José Alejandro del Valle Gálvez, “Las fronteras de la Unión – El *modelo europeo* de fronteras”, *Revista de Derecho Comunitario Europeo*, Vol. 6, No. 12, 2002, pp. 299-341.

- José Alejandro del Valle Gálvez, “Los refugiados, las fronteras exteriores y la evolución del concepto de frontera internacional”, *Revista de Derecho Comunitario Europeo*, No. 55, 2016, pp. 759-777.

- José Antonio Castillo Parrilla, “The Legal Regulation of Digital Wealth: Commerce, Ownership and Inheritance of Data”, *European Review of Private Law*, No. 5, 2021, pp. 807-830.

- José Martín y Pérez de Nanclares, “La ley de tratados y otros acuerdos internacionales: una nueva regulación para disciplinar una práctica internacional difícil de ignorar”, *Revista Española de Derecho Internacional*, Vol. 67, No. 1, 2015, pp. 13-60.

- Juan José Gonzalo Domenech, “Las decisiones de adecuación en el Derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados

por los estados miembros”, *Cuadernos de Derecho Transnacional*, No. 1, Vol. 11, 2019, pp. 350-371.

- Juan Santos Vara, “La transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos”, *Cuadernos de la Cátedra de Seguridad Salmantina*, No. 7, 2012, pp. 1-25.

- Juan Santos Vara, “The External Activities of AFSJ Agencies: The Weakness of Democratic and Judicial Controls”, *European Foreign Affairs Review*, Vol. 20, No. 1, 2015, pp. 115-136.

- Julia Van Dessel, “International Delegation and Agency in the Externalization Process of EU Migration and Asylum Policy: the Role of the IOM and the UNHCR in Niger”, *European Journal of Migration and Law*, 2019, pp. 435-458.

- Juliana Kokott and Christoph Sobotta, “The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR”, *International Data Privacy Law*, Vol. 3, No. 4, 2013, pp. 222-228.

- Karen Birchard, “Dublin Convention on handling of EU asylum seekers becomes law”, *The Lancet (British edition)*, Vol. 350, 1997, pp. 675-748.

- Katharina Meissner, “Democratizing EU External Relations: The European Parliament’s Informal Role in SWIFT, ACTA, and TTIP”, *European Foreign Affairs Review*, Vol. 21, No. 2, 2016, pp. 269-288.

- Kathleen Gutman, “The essence of the Fundamental Right to an Effective Remedy and to a fair Trial in the Case-Law of the Court of Justice of the European Union: The Best is Yet to Come”, *German Law Journal*, Vol. 20, No. 6, 2019, pp. 884-903.

- Kirill Belogubets, “The protection of personal data in the context of law enforcement: recent case law of the European Court of Human Rights”, *ERA Forum*, Vol. 22, 2021, pp. 231-243.

- Koen Lenaerts and Jean-Pascal Van Ypersele, “Le Principe de subsidiarité et son contexte”, *Cahiers de Droit Européen*, Vol. 30, No. 1-2, 1994, pp. 3-85.

- Koen Lenaerts, “Constitutionalism and the Many Faces of Federalism”, *The American Journal of Comparative Law*, Vol. 38, No. 2, 1990, pp. 205-263.

- Kristian P. Humble, “International law, surveillance and the protection of privacy”, *The International Journal of Human Rights*, Vol. 25, No. 1, 2021, pp. 1-25.

- Kristin Bergtora Sandvik, Maria Gabrielsen Jumbert, John Karlsrud and Mareile Kaufmann, “Humanitarian technology: a critical research agenda”, *International Review of the Red Cross*, Vol. 96, No. 893, 2014, pp. 219-242.

- Lama Mourand, "Transforming refugees into migrants: institutional change and the politics of international protection", *European Journal of International Relations*, 2019, pp. 1-27.
- Laura Drechsler, "Comparing LED and GDPR Adequacy: One Standard Two Systems", *Global Privacy Law Review*, 2020, pp. 93-103.
- Leese Matthias, "Fixing State Vision: Interoperability, Biometrics, and Identity Management in the EU", *Geopolitics*, 2020, pp. 1-21.
- Lilian Edwards and Michael Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For", *Duke Law & Technology Review*, No. 17, 2017, pp. 18-84.
- Lingjie Kong, "Data Protection and Transborder Data Flow in the European and Global Context", *European Journal of International Law*, Vol. 21, No. 2, 2010, pp. 441-456.
- Lode Van Outrive, "Historia del Acuerdo y del Convenio Schengen", *Revista CIDOB d'Afers Internacionals*, No. 53, 2001, pp. 46-61.
- Lokke Moerel, "The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?", *International Data Privacy Law*, No. 46, Vol. 1, 2011, pp. 28-46.
- Luigi Condorelli, "Il Giudice italiano e i trattati internazionali: Gli accordi self-executing e non self-executing nell'ottica della giurisprudenza", *Rivista di diritto internazionale privato e processuale: Studi e pubblicazioni*, No. 12, Padova, CEDAM, 1974.
- Luis Miguel Hinojosa Martínez, "¿Provocará la regla del consenso la destrucción de la OMC?", *ICE una política comercial para reconstruir la globalización*, No. 922, 2021, pp. 1-16.
- Luisa Marin, "The Cooperation Between Frontex and Third Countries in Information Sharing: Practices, Law and Challenges in Externalizing Border Control Functions", *European Public Law*, Vol. 26, No. 1, 2020, pp. 157-180.
- Maarten Den Heijer, Teun van Os van den Abeelen, and Antanina Maslyka, "On the Use and Misuse of Recitals in European Union Law", *Amsterdam Law School Research Paper*, No. 31, 2019, pp. 1-24.
- Madeleine Colvin, "The Schengen information System: a human rights audit", *European Human Rights Law Review*, No. 3, 2001, pp. 271-279.
- Manon Julicher, Marina Henriques, Aina Amat Blai, and Pasquale Policastro, "Protection of the EU Charter for Private Legal Entities and Public Authorities? The

Personal Scope of Fundamental Rights within Europe Compared”, *Utrecht Law Review*, Vol. 15, No. 1, 2019, pp. 1-25.

- Marc Amstutz, “In between worlds: Marleasing and the emergence of interlegality in legal reasoning”, *European Law Journal*, No. 6, Vol. 11, 2005, pp. 766-784.

- Marc Maresceau “Bilateral Agreements concluded by the European Community”, *Collected Courses of the Hague Academy of International Law*, Vol. 309, 2004, pp. 125-452.

- Marc Rotenberg and David Jacobs, “Updating the Law of Information Privacy: The New Framework of the European Union”, *Harvard Journal of Law & Public Policy*, No. 36, 2013, pp. 605-652.

- Marcello Carammia, Stefano Maria Iacus, and Teddy Wilkin, “Forecasting asylum-related migration flows with machine learning and data at scale”, *Scientific Report*, 2022.

- Marcus Klamert, “What We Talk About When We Talk About Harmonisation”, *Cambridge Yearbook of European Legal Studies*, No. 17, 2015, pp. 360-379.

- Marek Szydło, “Principles underlying independence of national data protection authorities: Commission v. Austria”, *Common Market Law Review*, 2013, Vol. 50, No. 6, pp. 1809-1826.

- Maria Fletcher, “Schengen, the European Court of Justice and Variable geometry under the Lisbon Treaty: Balancing the UK’s ‘Ins’ and ‘Outs’”, *The European Constitutional Law Review*, Vol. 5, No. 1, 2009, pp. 71-98.

- Mariona Illamola Dausà, “Hacia una gestión integrada de las fronteras: El Código de Fronteras Schengen y el cruce de fronteras en la Unión Europea”, *Barcelona Centre for International Affairs*, No. 15, 2008, pp. 148-179.

- Marise Cremona, “External Relations of the EU and the Member States: Competences, Mixed Agreements, International Responsibility, and Effect of International Law”, *EU Working Paper*, No. 22, 2006, pp. 1-40.

- Martin Abrams, John Abrams, Peter Cullen, and Lynn Goldstein, “Artificial Intelligence, Ethics, and Enhanced Data Stewardship”, *IEEE Security & Privacy*, Vol. 17, No. 2, 2019, pp. 17-30.

- Martin Weiler, "The Right to Privacy in the Digital Age: The Commitment to Human Rights Online", *German Yearbook of International Law*, No. 57, 2014, pp. 651-666.

- Marx, “Adjusting the Dublin Convention: New Approaches to Member States Responsibility for Asylum Applicants”, *European Journal of Migration and Law*, 2001, Vol. 3, No. 1, pp. 7-21.

- Mascia Toussaint, “EURODAC: un système informatisé européen de comparaison des empreintes digitales des demandeurs d’asile”, *Revue du marché commun et de l’Union Européenne*, No. 429, 1999, pp. 421-425.

- Matteo E. Bonfanti, “Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti”, *Diritti Umani e Diritto Internazionale*, Vol. 5, No. 3, 2011, pp. 437-481.

- Melanie Fink, “Frontex Working Arrangements: Legitimacy and Human Rights Concerns Regarding ‘Technical Relationship’”, *Utrecht Journal of International and European Law*, Vol. 28, No. 75, 2012, pp. 20-35.

- Merijn Chamon and Valerie Demedts, “Constitutional limits to the EU agencies’ external relations”, *TARN Working Paper*, No. 11, 2017, pp 1-22.

- Merijn Chamon, “A Constitutional Twilight Zone: EU Decentralized Agencies’ External Relations”, *Common Market Law Review*, No. 56, 2019, pp. 1509-1548.

- Merijn Chamon, “The Institutional Balance, an Ill-Fated Principle of EU Law?”, *European Public Law*, Vol. 21, No. 2, 2015, pp. 371-391.

- Michael Kirby, “The history, achievement and future of the 1980 OECD guidelines on privacy”, *International Data Privacy Law*, 2011, No. 1, Vol. 1, pp. 6-14.

- Micheal Yilma Kinfe, "The Right to Privacy in the Digital Age: Boundaries of the New UN Discourse", *Nordic Journal of International Law*, Vol. 87, No. 4, 2018, pp. 485-528.

- Michèle Finck and Frank Pallas, “They who must not be identified—distinguishing personal from non-personal data under the GDPR”, *International Data Privacy Law*, Vol. 10, No. 1, 2020, pp. 11-36.

- Michele Nino, “La sentenza Schrems II della Corte di Giustizia UE: trasmissione dei dati personali dell’Unione europea agli Stati terzi e tutela dei diritti dell’uomo”, *Diritti umani e Diritto internazionale*, 2020, Vol. 14, No. 3, pp. 733-760.

- Mikel Recuero Linares, “Transferencias internacionales de datos genéticos y datos de salud con fines de investigación”, *Revista de Derecho y Genoma Humano Genética, Biotecnología y Medicina Avanzada*, 2019, pp. 413-433.

- Mistale Taylor, “The EU’s human rights obligations in relation to its data protection laws with extraterritorial effect”, *International Data Privacy Law*, 2015, Vol. 5, No. 4, pp. 246-256.

- N. Cornago Proeto, “Elementos para el análisis del proceso político en los regímenes internacionales: el multilateralismo no necesariamente formalizado”, *Anuario Español de Derecho Internacional*, Vol. 15, 1999, pp. 205-234.

- Nicholas Grief, “EU Law and security”, *European Law Review*, No. 32, 2007, pp. 752-765.

- Niovi Vavoula, “Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism”, *European Journal of Migration and Law*, Vol. 23, No. 4, 2021, pp. 457-484.

- Niovi Vavoula, “Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?”, *European Public Law*, Vol. 26, No. 1, 2020, pp. 131-156.

- Norbert Reich, “Competition between Legal Orders: A New Paradigm of EC law?”, *Common Market Law Review*, Vol. 29, 1992, pp. 861-896.

- Orla Lynskey, “Deconstructing Data Protection: The Added-Value of a Right to Data Protection in the EU Legal Order”, *International and Comparative Law Quarterly*, Vol. 63, No. 3, 2014, pp. 569-598.

- Orla Lynskey, “The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland”, *Common Market Law Review*, Vol. 51, No. 6, 2014, pp. 1789-1811.

- Oscar Schachter, “International Law in Theory And Practice General Course in Public International Law”, *Collected Courses of the Hague Academy of International Law*, Vol. 178, 1982, pp. 9-396.

- Oscar Schachter's, “International Law in Theory and Practice General Course in Public International Law”, *Collected Courses of the Hague Academy of International Law*, Vol. 178, 1982, pp. 9-396.

- Özgür Heval Çınar, “The current case law of the European Court of Human Rights on privacy: challenges in the digital age”, *International journal of human rights*, Vol. 25, No. 1, 2021, pp. 26-51.

- Pablo Jesús Martín Rodríguez, “Crónica de una muerte anunciada: Comentario a la Sentencia del Tribunal de Justicia (Gran Sala) de 26 de febrero de 2013, Stefano Melloni, C-399/11”, *Revista General de Derecho Europeo*, No. 30, 2013, pp. 1-45.

- Pablo Jesús Martín Rodríguez, “La emergencia de los límites constitucionales de la confianza mutua en el espacio de libertad, seguridad y justicia en la Sentencia del Tribunal

de Justicia Aranyosi y Caldaru”, *Revista de Derecho Comunitario Europeo*, No. 20, Vol. 55, 2016, pp. 859-900.

- Pablo Jesús Martín Rodríguez, “Tribunal Constitucional -- Sentencia 26/2014, de 13 de febrero, en el recurso de amparo 6922-2008 promovido por Don Stefano Melloni”, *Revista de Derecho Comunitario Europeo*, No. 18, Vol. 48, 2014, pp. 603-622.

- Patricia L. Bellia, “Chasing Bits across Border”, *University of Chicago Legal Forum*, No. 1, Vol. 1, 2001, pp. 1-101.

- Paul De Hert and Serge Gutwirth, “Interoperability of police databases within the EU: An accountable political choice?”, *International Review of Law, Computers & Technology*, Vol. 20, No. 1-2, 2007, pp. 21-35.

- Paul M. Schwartz, “European Data Protection Law and Restrictions on International Data Flows”, *Iowa Law Review*, No. 80, pp. 471-496.

- Paul Roth, “Adequate Level of Data Protection in Third Countries Post-Schrems and under the General Data Protection Regulation”, *Journal of Law, Information and Science*, Vol. 25, No. 1, 2017, pp. 49-69.

- Paula García Andrade, “EU external competences in the field of migration: how to act externally when thinking internally”, *Common Market Law Review*, No. 55, 2018, pp. 157-200.

- Paula García Andrade, “La base jurídica de la celebración de acuerdos internacionales por parte de la UE: entre la PESC y la dimensión exterior del Espacio de Libertad, Seguridad y Justicia. Comentario a la sentencia del Tribunal de Justicia de 14 de junio de 2016, Asunto C-263/14, Parlamento c. Consejo”, *Revista General de Derecho Europeo*, No. 41, 2017, pp. 128-160.

- Paula García Andrade, “The EU Accession to the Geneva Convention Relating to the Status of Refugees: Legal Feasibility and Added Value”, *The Spanish Yearbook of International Law*, 2019, pp. 193-211.

- Paula J. Bruening, “Interoperability: analysing the current trends & developments”, *Data protection law & policy*, 2012, pp. 12-14.

- Pedro Alberto de Miguel Asensio, “Competition and applicable law in the General Data Protection Regulation of the European Union”, *Revista Española de Derecho Internacional*, No. 1, Vol. 69, 2017, pp. 75-108.

- Peter Hustinx, “EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation”, *Collected Courses of the European*

University Institute's Academy of European Law: 24 Session on European Union Law, 2013, pp. 1-52.

- Petr Popisil, "European Union External and Internal Humanitarian Aid", *European Food and Feed Law Review*, Vol. 14, No. 6, 2019, pp. 522-527.

- Raphael Gellert and Serge Gutwirth, "The legal construction of privacy and data protection", *Computer Law & Security Review*, No. 29, 2013, pp. 522-530.

- Renaud Dehousse, "Delegation of Powers in the European Union: The Need for a Multi-Principals Model", *West European Politics*, Vol. 31, No. 4, 2008, pp. 789-805.

- Riccardo Pisillo Mazzeschi, "Responsabilité de l'État pour violation des obligations positives relatives aux droits de l'homme", *Collected Courses of the Hague Academy of International Law*, Vol. 333, 2008, pp. 175-506.

- Robin S. S. Kramer, "Face morphing attacks: Investigating detection with humans and computers", *Cognitive Research: Principles and Implications*, Vol. 28, No. 4, 2019, pp. 1-15.

- Rolf H. Weber, "Transborder data transfers: concepts, regulatory approaches and new legislative initiatives", *International Data Privacy Law*, Vol. 3, No. 2, 2013, pp. 117-130.

- Rut Bermejo Casado, "El proceso de institucionalización de la cooperación en la gestión operativa de las fronteras externas de la UE", *Barcelona Centre for International Affairs*, No. 91, 2010, pp. 29-62.

- Santa Slokenberga, "Biobanking and data transfer between the EU and Cape Verde, Mauritius, Morocco, Senegal, and Tunisia: adequacy considerations and Convention 108", *International Data Privacy Law*, No. 2, Vol. 10, May 2020, pp. 132-145.

- Simon Robins, "The Affective Border: Missing Migrants and the Governance of Migrant Bodies at the European Union's Southern Frontier", *Journal of Refugee Studies*, 2019, pp. 1-19.

- Stephen McGarvey, "The 2006 EC Data Retention Directive: A Systematic Failure", *Hibernian Law Journal*, No. 10, 2011, pp. 119-171.

- Steve Peers, "The 'Opt-out' that Fell to Earth: The British and Polish Protocol Concerning the EU Charter of Fundamental Rights", *Human Rights Law Review*, Vol. 2, No. 2, 2012, pp. 375-389.

- Svetlana Yakovleva, "Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'", *Journal of World Investment & Trade*, Vol. 21, 2020, pp. 881-919.

- Tadas Klimas and Jflrate Vaitiukait, “The law of recitals in European Community legislation”, *ILSA Journal of International & Comparative Law*, No. 1, Vol. 15, 2008, pp. 61-93.

- Teresa Fajardo del Castillo, “Avances y retrocesos en materia de acuerdos mixtos y de acceso a la justicia para la protección del medio ambiente a la luz de la sentencia del tribunal de justicia de 8 de marzo de 2011 en el asunto oso pardo”, *Revista General de Derecho Europeo*, No. 29, 2013, pp. 1-27.

- Teresa Fajardo del Castillo, “El acuerdo de París sobre el cambio climático: sus aportaciones al desarrollo progresivo del derecho internacional y las consecuencias de la retirada de los Estados Unidos”, *Revista Española de Derecho Internacional*, No. 1, Vol. 70, 2018, pp. 23-51.

- Teresa Fajardo del Castillo, “El Pacto Mundial por una migración segura, ordenada y regular: un instrumento de soft law para una gestión de la migración que respete los derechos humanos”, *Revista electrónica de estudios internacionales*, No. 38, pp. 1697-5197.

- Teresa Fajardo del Castillo, “La directiva sobre el retorno de los inmigrantes en situación irregular”, *Revista de Derecho Comunitario Europeo*, No. 33, 2009, pp. 453-499.

- Teresa Quintel, “Interoperability of EU Databases and Access to Personal Data by National Police Authorities under Article 20 of the Commission Proposals”, *European Data Protection Law Review*, Vol. 4, No. 4, 2018, pp. 470-482.

- Teresa Quintel, “Interoperable Data Exchanges Within Different Data Protection Regimes: The Case of Europol and the European Border and Coast Guard Agency”, *European Public Law*, Vol. 26, No. 1, 2020, pp. 205-226.

- Theodor Meron, “International Law in the Age of Human Rights: General Course on Public International Law”, *The Hague Academy Collected Courses Online*, Vol. 301, 2003, pp. 9-490.

- Thierry Balzacq, Didier Bigo, Sergio Carrera, and Elspeth Guild, “Security and the Two-Level Game: The Treaty of Prüm, the EU and the Management of Threats”, *Centre for European Policies Studies Working Document*, No. 234, 2006, pp 21-38.

- Thomas Buergenthal, “Self-Executing and Non-Self-Executing Treaties”, *Collected Courses of The Hague Academy of International Law*, Vol. 235, pp. 303-400.

- Toptchiyska Denitza, “The Rule of Law and EU Data Protection Legislation: Some Controversial Issues in light of the new EU General Data Protection Regulation”, *The ORBIT Journal*, Vol. 1, No. 1, 2017, pp. 1-16.

- Troisi Emiliano, "AI e GDPR: L'Automated Decision Making, la Protezione dei Dati e il Diritto alla 'Intellegibilit ' dell'Algoritmo", *European Journal of Privacy Law & Technologies*, No. 41, 2019, pp. 41-59.

- Turgut Aythan Beydogan, "Interoperability-Centric Problems: New Challenges and Legal Solutions", *International Journal of Law and Information Technology*, Vol. 18, No. 4, 2010, pp. 301-331.

- Valeria Manzo, "The General Data Protection Regulation (GDPR) nella Pubblica Amministrazione", *European Journal of Privacy Law & Technologies*, Vol. 30, 2019, pp. 30-40.

- Valsamis Mitsilegas, "Immigration Control in an Era of Globalization: Deflecting Foreigners, Weakening Citizens, Strengthening the State", *Indiana Journal Global Legal Studies*, No. 3, Vol. 19, 2012, pp. 3-60.

- Vanmala Hiranandani, "Privacy and security in the digital age: contemporary challenges and future directions", *The International Journal of Human Rights*, Vol. 15, No. 7, 2011, pp. 1091-1106.

- Vincent Lecocq, "La convention de Schengen", *Defense National*, No. 3, 1992, pp. 91-99.

- Vlad Constantinesco, "Who's afraid of Subsidiarity?", *Yearbook of European Law*, Vol. 1, No. 1, 1991, pp. 67-97.

- Wachter Sandra, Mittelstadt Brent, and Floridi Luciano, "Why a right to explanation of automated decision- making does not exist in the GDPR", *International Data Privacy Law*, No. 2, 2017, pp. 76-99.

- Wenceslas de Lobkovic, "La Convention de Dublin: un utile complement au droit humanitaire international", *Objectif Europe*, No. 10, 1990, pp. 7-12.

- Werner Vandenbruwaene, "Multi-Level Governance through a Constitutional Prism", *Maastricht Journal of European and Comparative Law*, No. 2, Vol. 21, 2014, pp. 229-242.

- Winston J. Maxwell, "Principles-based regulation of personal data: the case of 'fair processing'", *International Data Privacy Law*, 2015, Vol. 5, No. 3, pp. 205-216.

- Yves Poullet, "Transborder Data Flows and Extraterritoriality: the European Position", *Journal of International Commercial Law and Technology*, Vol. 2, 2007, pp. 141-148.

Dissertation

- Claudio Matera, *The External Dimensions of the EU Area of Freedom, Security and Justice: A Constitutional Perspective*, Ph.D. dissertation, University of Twente, 2016.

- Elena María Torroglosa García, *Digital Identity Management Through the Interoperability of Heterogeneous Authentication and Authorization Infrastructures*, Ph.D. dissertation, University of Murcia, 2017.

- Fabrizio Carlo, *How can INTERPOL contribute to future border integrity?*, LL.M. dissertation, European Joint Master's in Strategic Border Management, University of Warsaw, 2017.

- Jorrit J. Rijpma, *Building Borders: The Regulatory Framework for the Management of the External Borders of the European Union*, Ph.D. dissertation, EUI (Fiesole), 2009.

- Oscar Aleixo Costa Rocha, *Adapting a System-Theoretic Hazard Analysis Method for Interoperability of Information Systems in Health Care*, LL.M. dissertation in Computer Science, University of Victoria.

- Teresa Fajardo del Castillo, *La política exterior de la Comunidad Europea en materia de medio ambiente*, Ph.D. dissertation, Granada, 2002.

Study

- Alexander Angers, Dafni Maria Kagkli, Laura Oliva, Mauro Petrillo, and Barbara Raffael, *Study on DNA Profiling Technology for its Implementation in the Central Schengen Information System*, Publications Office of the European Union, EUR 29766 EN, Luxembourg, 2019.

- Alexander Betts and James Milner, *The Externalization of EU Asylum Policy: The Position of African States*, Danish institute for international studies, Copenhagen, 2007.

- Didier Bigo, Sergio Carrera, Ben Hayes, Nicholas Hernanz, and Julien Jeandesboz, *Justice and Home Affairs Databases and a Smart Borders System at EU External Borders. An Evaluation of Current and Forthcoming Proposals*, Centre for European Policy Studies, Brussels, 2012.

- Didier Bigo, Sergio Carrera, Gloria González Fuster, Elspeth Guild, Paul de Hert, Julian Jeandesboz, and Dr Vagelis Papakonstantinou, *Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament*, Policy department C: Citizens' rights and constitutional affairs civil liberties, justice and home affairs, Brussels, 2011.

- Els Kindt and Lorenz Müller, *D3.10: Biometrics in identity management*, Future of Identity in the Information Society, Brussels/The Hague, 2007.

- European Parliament, *Developing a Criminal Justice Area in the European Union*, PE 493.043, Brussels, 2014.

- Francesco Ragazzi, Elif Mendos Kuskonmaz, Ildikó Z Pájás, Ruben van de Ven, and Ben Wagner, *Biometric & Behavioural Mass Surveillance in EU Member States*, Brussels, 2021.

- Global Research Centre, *INTERPOL: Red Notices*, Washington, Law Library of Congress, 2010.

- Guenter Schumacher, *Fingerprint Recognition for Children*, JRC Technical Reports, Brussels, 2013.

- Javier Galbally Herrero, Pasquale Ferrara, Rudolf Haraksim, Apostolos Psyllos, and Laurent BESLAY, *Study on Face Identification Technology for its Implementation in the Schengen Information System*, Publications Office of the European Union, EUR 29808 EN, Luxembourg, 2019.

- Jörg Monar, *The External Dimension of the EU's Area of Freedom, Security and Justice: Progress, potential and limitations after the Treaty of Lisbon*, Swedish Institute for European Policy Studies, 2012.

- Katharina Eisele, *Interoperability between EU information systems for security, border and migration management*, Initial Appraisal of a European Commission Impact Assessment, PE 615.649, Brussels, 2018.

- Laurent Beslay and Javier Galbally, *Fingerprint identification technology for its implementation in the Schengen Information System II (SIS-II)*, Publications Office of the European Union, EUR 27473 EN, Luxembourg, 2015.

- Laurent Beslay, Javier Galbally Herrero, and Rudolf Haraksim, *Automatic fingerprint recognition: from children to elderly. Ageing and age effects*, JRC Technical Report, Italy, 2018.

- Mara Wesseling, *An EU Terrorist Finance Tracking System*, Royal United Services Institute for Defence and Security Studies, United Kingdom, 2016.

- Mark Latonero, Keith Hiatt, Antonella Napolitano, Giulia Clericetti, and Melanie Penagos, *Digital Identity in the Migration & Refugee Context: Italy Case Study*, Italy, 2019.

- Meijers Committee standing committee of experts on international immigration, refugee and criminal law, *CM1802 Comments on the Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)*, Leiden, 2017.

- Mirja Gutheil, Quentin Liger, James Eager, Yemi Oviosu, and Daniel Bogdanovic, *Interoperability of Justice and Home Affairs Systems*, PE 604.947, Brussels, 2018.

- Niovi Vavoula and Valsamis Mitsilegas, *Strengthening Europol's mandate. A legal assessment of the Commission's proposal to amend the Europol Regulation*, European Parliament's Committee on Civil Liberties, Justice and Home Affairs, Brussels, 2021.

- Paul De Hert, *What are the risks and what guarantees need to be put in place in view of interoperability of police databases?*, IP/C/LIBE/FWC/2005-25, Brussels, 1.02.2006.

- Peter Hobbing, *An analysis of the commission communication (COM (2005) 597 final of 24.11.2005) on improved effectiveness, enhanced interoperability and synergies among European databases in the area of justice and home affairs*, IP/C/LIBE/FWC/2005-08, Brussels, 14.02.06.

- Peter Hobbing, *Briefing paper: An analysis of the commission communication (COM (2005) 597 final of 24.11.2005) on improved effectiveness, enhanced interoperability and synergies among European databases in the area of justice and home affairs*, IP/C/LIBE/FWC/2005-08, Brussels, 14.02.2006.

- Sergio Carrera, Gloria González Fuster, Elspeth Guild, and Valsamis Mitsilegas, *Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights*, Brussels, Centre of European Policy Studies, Brussels, 2015.

Blog

- Evelien Brouwer, "A Point of No Return in Purpose Limitation? Interoperability and the Blurring of Migration and Crime", *Blog Forum: Interoperable Information Systems in the EU Area of Freedom, Security and Justice*, the date is not specified, available at www.migrationpolicycentre.eu.

- Francesca Tassinari, "Privacy enhancing readmission: the clause on data protection in the EURAs", *ADiM Blog, Analyses & Opinions*, 30.06.2021, available at www.adimblog.com.

- Henrik Larsen, "What the Danish 'no' vote on Justice and Home Affairs means for Denmark and the EU", *LSE European Politics and Policy (EUROPP) Blog*, 10.12.2015, available at www.wprints.lse.ac.uk.

- Tomasz Dąbrowski, "The political complications of including Bulgaria and Romania in the Schengen Area", *Analyses*, 22.09.2021, available at www.osw.wae.pl.

- Violeta Moreno-Lax, "A New Common European Approach to Search and Rescue? Entrenching Proactive Containment", *EU Immigration and Asylum Law and Policy*, 3.02.2021, available at www.eumigrationlawblog.eu.

News

- “Accord entre le Parlement européen et la Présidence du Conseil de l'UE sur la nouvelle Agence européenne de l'asile”, *Bulletin Quotidien Europe*, No. 12751, Brussels, 29.06.2021.
- “Accord interinstitutionnel sur la réforme d'Europol”, *Bulletin Quotidien Europe*, No. 12881, 2.2.2022.
- “Accord PE/Conseil de l'UE sur le transfert du système informatique e- CODEX au siège de l'agence eu-LISA”, *Bulletin Quotidien Europe*, No. 12850, 10.12.2021.
- "Adéquation du régime britannique de protection des données personnelles, le PE demande à la Commission de revoir sa copie", *Bulletin Quotidien Europe*, No. 12724, 22.05.2021.
- “Application du RGPD, le manque d'harmonisation entre autorités nationales pointé par les eurodéputés”, *Bulletin Quotidien Europe*, No. 12915, 22.3.2022.
- "Conseil de l'UE et le PE s'accordent sur le rôle d'Europol dans l'introduction de nouvelles alertes dans le Système d'information Schengen", *Bulletin Quotidien Europe*, No. 12911, 16.3.2022.
- “DMA, les seuils de désignation et l'interopérabilité au cœur de l'accord provisoire entre le PE et le Conseil de l'UE”, *Bulletin Quotidien Europe*, No. 12919, 26.3.2022.
- “Droits de l'enfant, Parquet européen, migration et Afghanistan au menu des ministres de la Justice et de l'Intérieur de l'UE”, *Bulletin Quotidien Europe*, No. 12805, 6.10.2010.
- “Droits et principes numériques, la Présidence française du Conseil de l'UE met l'accent sur le respect des droits de l'Homme”, *Bulletin Quotidien Europe*, No. 12942, 30.4.2022.
- “eu-LISA and EASO Sign a Three-Year Cooperation Plan”, *Press Release*, 15.11.2020, available at www.eulisa.europa.eu.
- “eu-LISA and EC signed the Delegation Agreement on Smart Borders Pilot”, *Press Release*, 16.01.2015, available at www.eulisa.europa.eu.
- “eu-LISA and Eurojust Consolidate Their Cooperation in the Justice Domain”, *Press Release*, 11.10.2021, available at www.eulisa.europa.eu.
- “eu-LISA Headquarters Now in a Smart New House”, *Press Release*, 19.09.2018, available at www.eulisa.europa.eu.
- “eu-LISA signs Site Agreement with France”, 5 December 2013 and the “eu-LISA Inaugurates Its Operational Site’s New Building”, *Press Release*, 20.11.2018, available at www.eulisa.europa.eu.
- “eu-LISA Site Agreement ratified by the Estonian Parliament”, *Press Release*, 18.02.2015, available at www.eulisa.europa.eu

- “Eurojust demande plus de moyens pour renforcer ses effectifs”, *Bulletin Quotidien Europe*, No. 12881, 2.2.2022.
- “Europol peine à aider les États membres dans leur lutte contre les passeurs, selon la Cour des comptes européenne”, *Bulletin Quotidien Europe*, No. 12802, 1.10.2021.
- “Feu vert au nouvel accord sur les visas de court séjour avec le Cap-Vert”, *Bulletin Quotidien Europe*, No. 12781, 2.9.2021.
- “Feu vert des États membres à l’installation du système informatique e-CODEX à Tallinn”, *Bulletin Quotidien Europe*, No. 12767, 23.7.2021.
- “Intelligence artificielle et stratégie de données, les eurodéputés se penchent sur le sujet de la coopération international”, *Bulletin Quotidien Europe*, No. 12802, 1.10.2021.
- “Intelligence artificielle, les eurodéputés souhaitent une approche fondée sur le risqué”, *Bulletin Quotidien Europe*, No. 12410, 24.1.2020.
- “INTERPOL unveils new global database to identify missing persons through family DNA”, *News&Events*, 1.06.2021, available at www.interpol.int.
- “L’acheminement de l’aide d’urgence de l’UE à l’Ukraine et aux pays voisins monte en puissance”, *Bulletin Quotidien Europe*, No. 12911, 16.3.2022.
- “L’agence Europol déploie des équipes aux frontières de l’Ukraine”, *Bulletin Quotidien Europe*, No. 12924, 2.4.2022.
- “L’argent européen n’est pas destiné à financer des ‘murs’ anti- migrants aux frontières extérieures de l’UE, souligne la Commission”, *Bulletin Quotidien Europe*, No. 12808, 9.10.2021.
- “L’agence européenne pour la gestion opérationnelle des systèmes d’information planche sur la standardisation des données”, *Bulletin Quotidien Europe*, No. 12851, 11.12.2021.
- “L’Irlande rejoint le Système d’information Schengen”, *Bulletin Quotidien Europe*, No. 12678, 16.3.2021.
- “L’UE accroît son aide à l’Ukraine et aux pays voisins au moyen de la réserve d’équipements médicaux *RescEU* et de centres logistiques”, *Bulletin Quotidien Europe*, No. 12904, 5.3.2022.
- “L’UE annonce plus de 500 millions d’euros d’aide pour l’Ukraine et les pays voisins et poursuit la coordination des biens acheminés”, *Bulletin Quotidien Europe*, No. 12902, 3.3.2022.
- “La Commission européenne à nouveau questionnée sur son action après de nouvelles allégations de refoulements de migrants”, *Bulletin Quotidien Europe*, No. 12807, 8.10.2021.

- “La Commission européenne lance une consultation publique sur la numérisation des procédures d'acquisition de visas”, *Bulletin Quotidien Europe*, No. 12676, 12.3.2021.
- “La Commission européenne propose de durcir la délivrance de visas de court séjour pour les ressortissants de trois pays tiers”, *Bulletin Quotidien Europe*, No. 12763, 16.7.2021.
- “La commission européenne propose de renforcer le mandat d'Eurojust dans le contexte de crimes de guerre suspectés en Ukraine”, *Bulletin Quotidien Europe*, No. 12938, 26.4.2022.
- “La Commission européenne propose de renforcer les outils de coopération policière dans l'UE”, *Bulletin Quotidien Europe*, No. 12849, 9.12.2021.
- “La Commission européenne rappelle que la protection des données n’est pas un luxe, mais une nécessité”, *Bulletin Quotidien Europe*, No. 12412, 28.1.2020.
- “La plateforme d'enregistrement des déplacements de réfugiés ukrainiens dans l'UE ne sera pas prête avant fin mai”, *Bulletin Quotidien Europe*, No. 12935, 21.4.2022.
- “La Présidence française propose d'intégrer dans Eurodac les personnes secourues en mer ainsi que les réfugiés bénéficiant de la protection temporaire”, *Bulletin Quotidien Europe*, No. 12946, 6.5.2022.
- “La Présidence slovène constate des progrès sur la réforme d'Europol, mais des questions restent ouvertes sur les alertes Schengen et les droits fondamentaux”, *Bulletin Quotidien Europe*, No. 12859, 23.12.2021.
- “Le commissaire Thierry Breton inaugure à Luxembourg le siège de l’entreprise commune européenne pour le calcul à haute performance”, *Bulletin Quotidien Europe*, No. 12711, 4.5.2021.
- “Le Conseil de l'UE se penche sur le lien entre politique des retours et de réadmission, et utilisation de la politique des visas”, *Bulletin Quotidien Europe*, No. 12673, 9.3.2021.
- “Le Conseil donne son feu vert pour la signature du second protocole de la convention de Budapest sur la cybercriminalité”, *Bulletin Quotidien Europe*, No. 12926, 6.4.2022.
- “Le groupe Verts/ALE au PE appelle à la prudence concernant la surveillance biométrique et comportementale au sein des États membres”, *Bulletin Quotidien Europe*, No. 12819, 26.10.2021.
- “Le ministre de l'Intérieur slovène croit en une accession rapide de la Croatie à l'espace Schengen”, *Bulletin Quotidien Europe*, No. 12850, 10.12.2021.
- “Le Parlement européen confirme les nouvelles règles du Système d'information sur les visas”, *Bulletin Quotidien Europe*, No. 12757, 8.7.2021.

- “Le Parlement européen donne un avis positif sur quatre décisions du Conseil sur les échanges automatisés de données”, *Bulletin Quotidien Europe*, No.12918, 25.3.2022.
- “Le Parlement européen valide la constitution de sa commission d'enquête sur l'utilisation du logiciel espion Pegasus dans l'UE”, *Bulletin Quotidien Europe*, No. 12908, 11.3.2022.
- “Le PE appelle l'UE à intensifier son action dans le monde”, *Bulletin Quotidien Europe*, No. 12893, 18.2.2022.
- “Le PE approuve l'accord interinstitutionnel sur le règlement 'e-CODEX ’”, *Bulletin Quotidien Europe*, No. 1291, 25.3.2022.
- “Le sixième sommet entre l'Union européenne et l'Union africaine a posé les fondations d'un partenariat renforcé et pragmatique pour la prospérité des deux continents”, *Bulletin Quotidien Europe*, No. 12894, 19.2.2022.
- “Les élus de la commission des Libertés civiles du PE saisis des difficultés de Chypre à gérer les flux de migrants”, *Bulletin Quotidien Europe*, No. 12936, 22.4.2022.
- “Les États membres de l'UE adoptent leur mandat sur les nouvelles compétences dévolues à Europol”, *Bulletin Quotidien Europe*, No. 12752, Brussels, 1.07.2021.
- “Les États membres de l'UE devraient terminer l'année sans réaliser de percée sur le Pacte 'Asile et migration'”, *Bulletin Quotidien Europe*, No. 12848, 8.12.2021.
- “Les États membres de l'UE évoqueront avec les eurodéputés les difficiles négociations sur les preuves électroniques”, *Bulletin Quotidien Europe*, No. 12850, 10.12.2021.
- “Les États membres de l'UE valident la réforme du mécanisme d'évaluation Schengen”, *Bulletin Quotidien Europe*, No. 12940, 28.4.2022.
- “Les États membres demandent un réexamen plus large du règlement ‘GDPR’”, *Bulletin Quotidien Europe*, No. 12405, 17.1.2020.
- “Les États membres soutiennent la poursuite des accords sur les données PNR avec l'Australie et les Etats-Unis”, *Bulletin Quotidien Europe*, No. 12722, 20.5.2021.
- “Les États membres de l'UE s'engagent avec leurs partenaires de la zone indo-pacifique pour promouvoir la protection des données”, *Bulletin Quotidien Europe*, No. 12899, 26.2.2022.
- “Les ministres de l'Intérieur de l'UE auront un premier débat d'orientation le 3 mars sur la réforme du Code frontières Schengen”, *Bulletin Quotidien Europe*, No. 12897, 24.2.2022.
- “Les pays européens doivent changer d'urgence leurs politiques migratoires, avertit Dunja Mijatović”, *Bulletin Quotidien Europe*, No. 12674, 10.3.2021.

- “Libéralisation des visas, les ressortissants moldaves, géorgiens et ukrainiens posent des difficultés à certains États membres”, *Bulletin Quotidien Europe*, No. 12801, 30.9.2021.
- “‘Mieux légiférer’, les États membres soutiennent globalement l’approche ‘One in, one out’”, *Bulletin Quotidien Europe*, No. 12802, 1.10.2021.
- “Manfred Weber estime que le budget européen doit pouvoir financer des clôtures anti-migrants”, *Bulletin Quotidien Europe*, No. 12821, 28.10.2021.
- “Mis en cause par l'OLAF et des enquêtes de presse sur les pratiques de refoulement, Fabrice Leggeri quitte la tête de l'agence Frontex”, *Bulletin Quotidien Europe*, No. 12942, 30.4.2022.
- “New documents reveal Europol’s plans to increase surveillance”, *EDRi*, 24.08.2016, available at www.edri.org.
- “Réseaux de passeurs, la Commission veut sanctionner les pays tiers qui instrumentalisent la migration”, *Bulletin Quotidien Europe*, No. 12801, 30.9.2021.
- “Sylvie Guillaume désignée rapporteur sur la réforme du Code frontières Schengen”, *Bulletin Quotidien Europe*, No. 12912, 17.3.2022.
- “The United Kingdom connected to SIS managed by eu-LISA”, *Press Release*, 13.04.2015, available at www.eulisa.europa.eu.
- “Transfert et protection des données, la Commission annonce un accord de principe sur un nouveau cadre avec les États-Unis”, *Bulletin Quotidien Europe*, No. 12919, 26.3.2022.
- “Un budget humanitaire solide et flexible, une priorité du Parlement européen pour l'action humanitaire future de l'UE”, *Bulletin Quotidien Europe*, No. 12855, 17.12.2021.
- “Une trentaine d'ONG s'inquiètent de la future base de données Eurodac sur les demandeurs d'asile”, *Bulletin Quotidien Europe*, No. 12787, 10.9.2021.
- “Vote on Eurodac planned for mid-November in Committee on Civil Liberties”, *Bulletin Quotidien Europe*, No. 12789, 13.09.2021.
- Ariel Bogle, “Biometric data is increasingly popular in aid work, but critics say it puts refugees at risk”, *ABC Science*, 21.06.2019, available at www.abc.net.
- Ayang Macdonald, “IDnow, INTERPOL pair up on fraud prevention training”, *BIOMETRICUPDATE.COM*, 21.03.2022, available at www.biometricupdate.com.
- Ben Perker, “Aid’s cash revolution: a numbers game”, *The New Humanitarian*, 2.11.2016, available at www.thenewhumanitarian.org.
- Chris Burt, “DHS to store tens of thousands of refugee biometric records from UNHCR”, *BIOMETRICUPDATE.COM*, 21.08.2019, available at www.biometricupdate.com.

- Chris Burt, “EU Parliament approved unified biometric and bio database of 350 million people”, *BIOMETRICUPDATE.COM*, 4.22.2019, available at www.biometricupdate.com.
- Chris Burt, “Nigeria moves to implement biometric ECOWAS card with \$41M MoU”, *BIOMETRICUPDATE.COM*, 25.04.2019, available at www.biometricupdate.com.
- Chris Burt, “Red Cross Norway tender seeks digital ID help for humanitarian aid”, in *BIOMETRICUPDATE.COM*, 17.07.2019, available at www.biometricupdate.com.
- Chris Burt, “UNHCR reaches 7.2M biometric records but critics express concern”, *BIOMETRICUPDATE.COM*, 24.06.2019, available at www.biometricupdate.com.
- Chris Burt, “UNHCR works toward self-managed refugee identity with biometrics to improve settlement outcomes”, in *BIOMETRICUPDATE.COM*, 20.09.2019.
- Euronews, “Red Cross' cyber attack exposes data of 515,000 vulnerable people”, *euronews*, 21.01.2020, available at www.euronews.com.
- European Commission, “Olaf and Eurojust sign memorandum of understanding”, *Press Release*, Brussels, 14.04.2003.
- European Council on Refugees and Exiles, “UK: NHS to Pull out of Data- Sharing Agreement with Home Office”, *ECRE Weekly Bulletin*, 16.11.2018, available at www.ecre.org.
- IOM, “European Commission and European External Action Service Strengthen Partnership”, *NEWS GLOBAL*, 15.07.2012, available at www.iom.int.
- IOM, “European Readmission Capacity Building Facility – EURCAP”, the date is not specified, available at <https://eea.iom.int>.
- IOM, “UNHCR Adapting to Modern Complexities of Resettlement, Mixed Migration Flows”, *Press Release*, 12.18.2019, available at www.iom.int.
- Jacques Semmelman and Emily Spencer Munso, “Interpol Red Notices and Diffusions: Powerful — And Dangerous — Tools of Global Law Enforcement”, *The Champion*, 2014, available at www.nacdl.org.
- Les eurodéputés confirment un premier accord sur la réforme d'Europol”, *Bulletin Quotidien Europe*, No. 12913, 18.3.2022.
- Lorraine Finlay, “Explainer: what is an Interpol red notice and how does it work?”, *The Conversation*, 30.01.2019, available at www.theconversation.com.
- Luana Pascu, “UNHCR to hire Interoperability Coordinator for biometric program”, *BIOMETRICUPDATE.COM*, 8.09.2019, available at www.biometricupdate.com.

- Pascale Davies, “Meta warns it may shut Facebook in Europe but EU leaders say life would be ‘very good’ without it”, *euronews.next*, 9.02.2022, available at www.euronews.com.

- Sikhulile Dhlamini, “Technology Allows Migrant Returnees in Hargeisa to Access Services”, *News - Global*, 19.07.2019, available at www.iom.int.

- UNHCR, “Data of millions of refugees now securely hosted in PRIMES”, *UNHCR Blogs*, 28.01.2019, available at www.unhcr.org.

- Vincent Manancourt, “EU, US strike preliminary deal to unlock transatlantic data flows”, *POLITICO*, 25.03.2022.

Law

United Nations

- Cartagena Protocol to the Convention on Biological Diversity, of 29 January 2000, Montreal on 29 January 2000, entered into force on 11 September 2003, *U.N.T.S.* Vol. 2226, p. 208.

- Chemical Convention No. 170 signed in Geneva on 25 June 1990, entered into force on 4 November 1993.

- Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters signed in Aarhus on 25 June 1998, entered into force on 30 October 2001, *U.N.T.S.* Vol. 2161, p. 447.

- Convention on Future Multilateral Cooperation in Northeast Atlantic Fisheries, signed in Ottawa on 24 October 1978, entered into force on 1 January 1979, *U.N.T.S.* No. 1799, Vol. 157, p. 369.

- Convention on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, signed in Prüm on 27 May 2005, entered into force on 1 November 2006.

- Convention relating to the Status of Refugees signed in Geneva on 28 July 1951, entered into force on 22 April 1954, *U.N.T.S.* No. 2545, Vol. 189, p. 137.

- International Convention on Civil and Political Rights, signed in New York on 16 December 1966, entered into force on 23 March 1976, *U.N.T.S.* Vol. 999, p. 171, and Vol. 1057, p. 407.

- Optional Protocol to the International Covenant on Civil and Political Rights, signed in New York on the 16 December 1966, entered into force on 23 March 1976, *U.N.T.S.* Vol. 999, p. 171.

- Second Optional Protocol to the International Covenant on Civil and Political Rights, aiming at the abolition of the death penalty, signed in New York on 15 December 1989, entered into force on 11 July 1991, *U.N.T.S.* Vol. 1642, p. 414.

- Vienna Convention on the Law of Treaties, signed in Vienna on 23 May 1969, entered into force on 27 January 1980, *U.N.T.S.* Vol. 1155, p. 331.

- Vienna Convention on the Law of Treaties between States and International Organizations or between International Organizations signed in Vienna on 21 March 1986.

Council of Europe

- Amending Protocol according to Article 4(2) of the Amendments approved by the Committee of Ministers of 15 June 1999.

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *ETS* 108, signed in Strasbourg on 28 January 1981, entered into force on 1 October 1985.

- European Convention on Human Rights, *CETS* 005, signed in Rome on 4 November 1950, entered into force on 3 September 1953.

- First Additional Protocol for the Protection of Individuals with regard to Automatic Processing of Personal Data to the Supervisory Authorities and cross-border data flows, *ETS* No. 181, signed in Strasbourg on 8 November 2001 and entered into force on 1 July 2004.

- Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *CETS* 223, signed in Strasbourg on 10 October 2018.

- Protocol No 15 amending the Convention on the Protection of Human Rights and Fundamental Freedoms, *ETS* 213, signed in Brussels on 24 June 2013, entered into force on 1 August 2021.

European Union

- Act concerning the conditions of accession of the Republic of Bulgaria and Romania and the adjustments to the Treaties on which the European Union is founded, *OJ L* 157, 21.6.2005, pp. 203-375.

- Act concerning the conditions of accession of the Republic of Croatia and the adjustments to the Treaty on European Union, the Treaty on the Functioning of the European Union and the Treaty establishing the European Atomic Energy Community, *OJ L* 112, 24.4.2012, pp. 6-110.

- Agreement between the European Community and the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State

responsible for examining a request for asylum lodged in a Member State or in Iceland or Norway, *OJ L 93*, 3.4.2001, p. 40.

- Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland, *OJ L 53*, 27.2.2008, p. 5.

- Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, *OJ L 186*, 14.7.2012, pp. 4-16.

- Agreement between the European Union and Japan on mutual legal assistance in criminal matters, *OJ L 39*, 12.2.2010, pp. 20-35.

- Agreement between the European Union and the Republic of Moldova on operational activities carried out by the European Border and Coast Guard Agency in the Republic of Moldova, ST/7204/2022/INIT, *OJ L 91*, 18.3.2022, pp. 4-21.

- Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, *OJ L 8*, 13.1.2010, pp. 11-16.

- Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, *OJ L 336*, 10.12.2016, pp. 3-13.

- Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latter's association with the implementation, application and development of the Schengen *acquis*, *OJ 176/36*, 10.7.1999.

- Agreement establishing an Association between the European Economic Community and Turkey, signed at Ankara on 12 September 1963 by the Republic of Turkey, of the one part, and by the Member States of the EEC and the Community, of the other part, and concluded, approved and confirmed on behalf of the Community by Council Decision 64/732/EEC of 23 December 1963, *OJ 1973*, C 113, p. 1.

- Agreement on extradition between the European Union and the United States of America, *OJ L 181*, 19.7.2003, pp. 27-33.

- Agreement on mutual legal assistance between the European Union and the United States of America, *OJ L 181*, 19.7.2003, pp. 34-42.

- Agreement on the accession of the Kingdom of Denmark to the convention implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks

at the common borders signed at Schengen on 19 June 1990, *OJ L 239*, 22.9.2000, pp. 97-105.

- Agreement on the European Economic Area - Final Act - Joint Declarations - Declarations by the Governments of the Member States of the Community and the EFTA States - Arrangements - Agreed Minutes - Declarations by one or several of the Contracting Parties of the Agreement on the European Economic Area, *OJ L 1*, 3.1.1994, pp. 3-522.

- Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community 2019/C 384 I/01, XT/21054/2019/INIT, *OJ C 384I*, 12.11.2019, pp. 1-177.

- Charter of Fundamental Rights of the European Union, *OJ C 326*, 26.10.2012, pp. 391-407.

- Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance), *OJ L 215*, 25.8.2000, pp. 7-47.

- Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, *OJ L 181*, 04.07.2001, pp. 19-31,

- Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection, *OJ L 235*, 6.7.2004, pp. 11-22.

- Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, *OJ L 385*, 29.12.2004, pp. 74-84.

- Commission Decision 2006/253/EC of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency (notified under document number C(2005) 3248) (Text with EEA relevance), *OJ L 91*, 29.3.2006, pp. 49-60.

- Commission Decision 2010/87 of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, *OJ L 39*, 12.2.2010, pp. 5-18.

- Commission Decision 85/410/EEC of 12 July 1985 relating to a proceeding under Article 85 of the TEEC (IV/4.204 Velcro/Aplix) (Only the French text is authentic), *OJ L* 233, 30.8.1985, pp. 22-32.

- Commission Decision of 17 June 2016 setting up the high-level expert group on information systems and interoperability C/2016/3780, *OJ C* 257, 15.7.2016, pp. 3-6.

- Commission Delegated Decision (EU) 2019/969 of 22 February 2019 on the tool enabling applicants to give or withdraw their consent for an additional retention period of their application file pursuant to Article 54(2) of Regulation (EU) 2018/1240 of the European Parliament and of the Council (Text with EEA relevance), C/2019/1532, *OJ L* 156, 13.6.2019, pp. 10-14.

- Commission Delegated Decision (EU) 2019/970 of 22 February 2019 on the tool for applicants to check the status of their applications and to check the period of validity and status of their travel authorisations pursuant to Article 31 of Regulation (EU) 2018/1240 of the European Parliament and of the Council (Text with EEA relevance), C(2019)1533, *OJ L* 156, 13.6.2019, pp. 15-19.

- Commission Delegated Decision (EU) 2019/971 of 26 February 2019 on the definition of the requirements of the secure account service pursuant to Article 6(4) of Regulation (EU) 2018/1240 of the European Parliament and of the Council, enabling applicants to provide any additional information or documentation required (Text with EEA relevance), C(2019)1695, *OJ L* 156, 13.6.2019, pp. 20-24

- Commission delegated decision of 10.12.2020 supplementing Regulation (EU) 2018/1240 of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) as regards flagging, COM(2020) 8709 final, Brussels, 10.12.2020.

- Commission Delegated Regulation (EU) 2021/2104 of 19 August 2021 laying down detailed rules on the operation of the web portal, pursuant to Article 49(6) of Regulation (EU) 2019/817 of the European Parliament and of the Council, C/2021/5050, *OJ L* 429, 1.12.2021, pp. 72-78.

- Commission Delegated Regulation (EU) 2021/2223 of 30 September 2021 supplementing Regulation (EU) 2019/817 of the European Parliament and of the Council with detailed rules on the operation of the central repository for reporting and statistics, C/2021/4982, *OJ L* 448, 15.12.2021, pp. 7-13.

- Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the

protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance) C/2016/4176, *OJ L* 207, 1.8.2016, pp. 1-112.

- Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2016) 8471) (Text with EEA relevance), C/2016/8471, *OJ L* 344, 17.12.2016, pp. 100-101.

- Commission Implementing Decision (EU) 2017/1528 of 31 August 2017 replacing the Annex to Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) (notified under document C(2017) 5893) C/2017/5893, *OJ L* 231, 7.9.2017, pp. 6-51.

- Commission Implementing Decision (EU) 2018/1547 of 15 October 2018 laying down the specifications for the connection of the central access points to the Entry/Exit System (EES) and for a technical solution to facilitate the collection of data by Member States for the purpose of generating statistics on the access to the EES data for law enforcement purposes, C/2018/662, *OJ L* 259, 16.10.2018, pp. 35-38.

- Commission Implementing Decision (EU) 2018/1548 of 15 October 2018 laying down measures for the establishment of the list of persons identified as overstayers in the Entry-Exit System (EES) and the procedure to make that list available to Member States, C/2018/6665, *OJ L* 259, 16.10.2018, pp. 39-42.

- Commission Implementing Decision (EU) 2019/326 of 25 February 2019 laying down measures for entering the data in the Entry/Exit System (EES), C/2019/1210, *OJ L* 57, 26.2.2019, pp. 5-9.

- Commission Implementing Decision (EU) 2019/329 of 25 February 2019 laying down the specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the Entry/Exit System (EES), C/2019/1280, *OJ L* 57, 26.2.2019, pp. 18-28.

- Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information (Text with EEA relevance) C/2019/304/, *OJ L* 76, 19.3.2019, pp. 1-58.

- Commission Implementing Decision 2013/115/EU of 26 February 2013 on the Sirene Manual and other implementing measures for the second generation Schengen Information System (SIS II) (notified under document C(2013) 1043), *OJ L* 71, 14.3.2013, pp. 1-36.

- Commission Implementing Decision 2019/1765 of 22 October 2019 providing the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth, and repealing Implementing Decision 2011/890/EU (notified under document C(2019) 7460) (Text with EEA relevance) C/2019/7460, *OJ L* 270, 24.10.2019, pp. 83-93.

- Commission implementing decision of 17.12.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act, C(2021) 9316 final, Brussels, 17.12.2021.

- Commission implementing decision pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, C(2021) 4801 final, Brussels, 28.06.2021.

- Commission Implementing Decision, laying down the technical specifications regarding the standards for security features and biometrics in passports and travel documents issued by Member States and repealing Decisions C(2006) 2909 and C(2008) 8657, C(2018) 7774 final, Brussels, 30.11.2018.

- Commission Implementing Regulation (EU) 2021/2225 of 16 November 2021 laying down the details of the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum quality standards for storage of data, pursuant to Article 37(4) of Regulation (EU) 2019/817 of the European Parliament and of the Council, C/2021/6719, *OJ L* 448, 15.12.2021, pp. 23-31.

- Commission Regulation (EC) No 1560/2003 of 2 September 2003 laying down detailed rules for the application of Council Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, *OJ L* 222, 5.9.2003, pp. 3-23.

- Common Consular Instructions on visas for the diplomatic missions and consular posts, *OJ C* 313, 16.12.2002, pp. 1-96.

- Consolidated version of the 1992 Treaty of the European Community, *OJ C* 224, 31.8.1992, pp. 6-79.

- Consolidated version of the Treaty on European Union, *OJ C* 326, 26.10.2012, pp. 13-390.
- Consolidated version of the Treaty on the Functioning of the European Union, *OJ C* 326, 26.10.2012, pp. 47-390.
- Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention), *OJ C* 316, 27.11.1995, pp. 1-32.
- Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities - Dublin Convention, *OJ C* 254, 19.8.1997, pp. 1-12.
- Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities, *OJ C* 254, 19.8.1997, pp. 1-12.
- Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, *OJ L* 239, 22.9.2000, pp. 19-62.
- Convention on the establishment of a European Police Office (Europol Convention), *OJ C* 316, 27.11.1995, pp. 2-32.
- Council Act of 12 March 1999 adopting the rules governing the transmission of personal data by Europol to third States and third bodies, *OJ C* 088, 30.03.1999, pp. 1-3.
- Council Act of 27 November 2003 drawing up, on the basis of Article 43 (1) of the Convention on the Establishment of a European Police Office (Europol Convention), a Protocol amending that Convention, *OJ C* 2, 06.01.2004, p. 1.
- Council Act of 28 February 2002 amending the Council Act of 12 March 1999 adopting the rules governing the transmission of personal data by Europol to third States and third bodies, *OJ C* 58, 5.3.2002, p. 12.
- Council Act of 28 November 2002 drawing up a Protocol amending the Convention on the establishment of a European Police Office (Europol Convention) and the Protocol on the privileges and immunities of Europol, the members of its organs, the deputy directors and the employees of Europol, *OJ C* 312, 16.12.2002, p. 1.
- Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, *OJ C* 197, 12.7.2000, pp. 1-2.

- Council Act of 3 November 1998 laying down rules concerning the receipt of information by Europol from third parties, *OJ C* 26, 30.1.1999, pp. 17-18.

- Council Act of 30 November 2000 drawing up, on the basis of Article 43(1) of the Convention on the establishment of a European Police Office (Europol Convention), a Protocol amending Article 2 and the Annex to that Convention, *OJ C* 358, 13.12.2000, p. 1.

- Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with International Criminal Police Organization, *OJ L* 27, 29.1.2005, pp. 61-62.

- Council Decision (EU) 2018/1600 of 28 September 2018 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis relating to the European Union Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), ST/12040/2018/INIT, *OJ L* 267, 25.10.2018, pp. 3-5.

- Council Decision (EU) 2019/267 of 12 February 2019 on the conclusion of the Status Agreement between the European Union and the Republic of Albania on actions carried out by the European Border and Coast Guard Agency in the Republic of Albania, ST/10302/2018/INIT, *OJ L* 46, 18.2.2019, pp. 1-2.

- Council Decision (EU) 2019/682 of 9 April 2019 authorising Member States to ratify, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ST/10923/2018/INIT, *OJ L* 115, 2.5.2019, pp. 7-8.

- Council Decision (EU) 2020/729 of 26 May 2020 on the conclusion of the Status Agreement between the European Union and Montenegro on actions carried out by the European Border and Coast Guard Agency in Montenegro, ST/6847/2019/REV/1, *OJ L* 173, 3.6.2020, pp. 1-2.

- Council Decision 1999/307/EC of 1 May 1999 laying down the detailed arrangements for the integration of the Schengen Secretariat into the General Secretariat of the Council, *OJ L* 119, 7.5.1999, pp. 49-52.

- Council Decision 1999/435/EC of 20 May 1999 concerning the definition of the Schengen acquis for the purpose of determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the acquis, *OJ L* 176, 10.7.1999, pp. 1-16.

- Council Decision 1999/436/EC of 20 May 1999 determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on

European Union, the legal basis for each of the provisions or decisions which constitute the Schengen *acquis*, *OJ L* 176, 10.7.1999, pp. 17-30.

- Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis*, *OJ L* 176, 10.7.1999, pp. 31-33.

- Council Decision 1999/437/EC with Iceland and Norway were made applicable to Switzerland already in, and the Council Decision 2011/842/EU of 13 December 2011 on the full application of the provisions of the Schengen *acquis* in the Principality of Liechtenstein, *OJ L* 334, 16.12.2011, pp. 27-28.

- Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis*, *OJ L* 131, 1.6.2000, pp. 43-47.

- Council Decision 2001/886/JHA of 6 December 2001 on the development of the second generation Schengen Information System (SIS II), *OJ L* 328, 13.12.2001, pp. 1-3.

- Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, *OJ L* 63, 6.3.2002, pp. 1-13.

- Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis*, *OJ L* 64, 7.3.2002, pp. 20-23.

- Council Decision 2002/463/EC of 13 June 2002 adopting an action programme for administrative cooperation in the fields of external borders, visas, asylum and immigration (ARGO programme), *OJ L* 161, 19.6.2002, p. 11.

- Council Decision 2003/659/JHA of 18 June 2003 amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, *OJ L* 245, 29.9.2003, pp. 44-45.

- Council Decision 2004/191/EC of 23 February 2004 setting out the criteria and practical arrangements for the compensation of the financial imbalances resulting from the application of Directive 2001/40/EC on the mutual recognition of decisions on the expulsion of third-country nationals, *OJ L* 60, 27.2.2004, pp. 55-57.

- Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, *OJ L* 183, 20.5.2004, p. 83.

- Council Decision 2004/867/EC of 13 December 2004 amending Decision 2002/463/EC adopting an action programme for administrative cooperation in the fields of external borders, visas, asylum and immigration, *OJ L* 371, 18.12.2004, pp. 48-49.

- Council Decision 2004/926/EC of 22 December 2004 on the putting into effect of parts of the Schengen acquis by the United Kingdom of Great Britain and Northern Ireland, *OJ L* 395, 31.12.2004, pp. 70-80.

- Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, *OJ L* 68, 15.3.2005, pp. 44-48.

- Council Decision 2005/511/JHA of 12 July 2005 on protecting the euro against counterfeiting, by designating Europol as the Central Office for combating euro counterfeiting, *OJ L* 185, 16.7.2005, pp. 35-36.

- Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences, *OJ L* 253, 29.9.2005, pp. 22-24.

- Council Decision 2006/1007/JHA of 21 December 2006 amending Decision 2001/886/JHA on the development of the second generation Schengen Information System (SIS II), *OJ L* 411, 30.12.2006, pp. 78-81.

- Council Decision 2006/230/EC of 18 July 2005 on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of API/PNR data Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data, *OJ L* 82, 21.3.2006, pp. 14-19.

- Council Decision 2006/688/EC of 5 October 2006 on the establishment of a mutual information mechanism concerning Member States' measures in the areas of asylum and immigration, *OJ L* 283, 14.10.2006, pp. 40-43.

- Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), *OJ L* 205, 7.8.2007, pp. 63-84.

- Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime, *OJ L* 332, 18.12.2007, pp. 103-105.

- Council Decision 2008/421/EC of 5 June 2008 on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Swiss Confederation, *OJ L* 149, 7.6.2008, pp. 74-77.

- Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, *OJ L* 210, 6.8.2008, pp. 1-11.

- Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, *OJ L* 218, 13.8.2008, pp. 129-136.

- Council Decision 2008/839/JHA of 24 October 2008 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II), *OJ L* 299, 8.11.2008, pp. 43-49.

- Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, *OJ L* 93, 7.4.2009, pp. 33-48.

- Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, *OJ L* 138, 4.6.2009, pp. 14-3.

- Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes, *OJ L* 323, 10.12.2009, pp. 20-30.

- Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information, *OJ L* 325, 11.12.2009, pp. 6-11.

- Council Decision 2009/935/JHA of 30 November 2009 determining the list of third States and organisations with which Europol shall conclude agreements, *OJ L* 325, 11.12.2009, pp. 12-13.

- Council Decision 2010/779/EU of 14 December 2010 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis relating to the establishment of a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, *OJ L* 333, 17.12.2010, p. 58.

- Council Decision 2011/352/EU of 9 June 2011 on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Principality of Liechtenstein, *OJ L* 160, 18.6.2011, pp. 84-87.

- Council Decision 2012/381/EU of 13 December 2011 on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of

Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, *OJ L* 186, 14.7.2012, p. 3.

- Council Decision 2012/472/EU of 26 April 2012 on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, *OJ L* 82, 21.3.2006, pp. 14-19.

- Council Decision 2013/392/EU of 22 July 2013 fixing the date of effect of Decision 2008/633/JHA concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, *OJ L* 198, 23.7.2013, pp. 45-46.

- Council Decision of 20 May 1999 concerning the definition of the Schengen acquis for the purpose of determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the acquis, *OJ L* 176/1, 10.7.1999, pp. 1-16.

- Council Decision of 28 January 2008 on the conclusion on behalf of the European Union of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis, *OJ L* 53, 27.2.2008, pp. 50-51.

- Council Decision of 6 April 2009 establishing the European Police Office (Europol), *OJ L* 121, 15.5.2009, pp. 37-66.

- Council Directive 2001/40/EC on the mutual recognition of decisions on the expulsion of third country nationals, *OJ L* 149, 2.6.2001, p. 34.

- Council Directive 2002/90/EC of 28 November 2002 defining the facilitation of unauthorised entry, transit and residence, *OJ L* 328, 5.12.2002, pp. 17-18.

- Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, *OJ L* 261, 6.8.2004, pp. 24-27.

- Council Directive 68/360/EEC of 15 October 1968 on the abolition of restrictions on movement and residence within the Community for workers of Member States and their families, *OJ L* 257, 19.10.1968, pp. 13-16.

- Council Directive 92/43/EEC of 21 May 1992 on the conservation of natural habitats and of wild fauna and flora, *OJ L* 206, 22.7.1992, pp. 7-50.

- Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, *OJ L* 190, 18.7.2002, pp. 1-20.

- Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence, *OJ L* 196, 2.8.2003, pp. 45-55.

- Council Framework Decision 2005/214/JHA of the 24 February 2005 on the application of the principle of mutual recognition to financial penalties as amended by Council Framework Decision 2009/299/JHA of 26 February 2009, *OJ L* 76, 22.3.2005, pp. 16-30.

- Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *OJ L* 69, 16.3.2005, pp. 67-71.

- Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, *OJ L* 386, 29.12.2006, pp. 89-100.

- Council Framework Decision 2008/675/JHA on taking account of convictions in the Member States of European Union in the course of new criminal proceedings, *OJ L* 220, 15.8.2008.

- Council Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union, as amended by Council Framework Decision 2009/299/JHA of 26 February 2009, *OJ L* 327, 5.12.2008, pp. 27-46.

- Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *OJ L* 350, 30.12.2008, pp. 60-71.

- Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters, *OJ L* 350, 30.12.2008, pp. 72-92.

- Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, *OJ L* 93, 7.4.2009, pp. 23-32.

- Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, PE/87/2018/REV/1, *OJ L* 151, 7.6.2019, pp. 143-150.

- Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings, *OJ L* 328, 15.12.2009, pp. 42-47.

- Council Framework Decision of 13 June 2002 on joint investigation teams, *OJ L* 162, 20.6.2002, pp. 1-3.

- Council Implementing Decision (EU) 2015/1956 of 26 October 2015 fixing the date of effect of Decision 2008/633/JHA concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, *OJ L* 284, 30.10.2015, pp. 146-148.

- Council Implementing Decision (EU) 2015/215 of 10 February 2015 on the putting into effect of the provisions of the Schengen acquis on data protection and on the provisional putting into effect of parts of the provisions of the Schengen acquis on the Schengen Information System for the United Kingdom of Great Britain and Northern Ireland, *OJ L* 36, 12.2.2015, pp. 8-10.

- Council Implementing Decision (EU) 2020/1745 of 18 November 2020 on the putting into effect of the provisions of the Schengen acquis on data protection and on the provisional putting into effect of certain provisions of the Schengen acquis in Ireland, *OJ L* 393, 23.11.2020, pp. 3-11.

- Council Regulation (EC) 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, *OJ L* 349, 25.11.2004, pp. 1-11.

- Council Regulation (EC) 377/2004 of 19 February 2004 on the creation of an immigration liaison officers network, *OJ L* 64, 2.3.2004, pp. 1-4.

- Council Regulation (EC) No 1091/2001 of 28 May 2001 on freedom of movement with a long-stay visa, *OJ L* 150, 6.6.2001, pp. 4-5.

- Council Regulation (EC) No 1104/2008 of 24 October 2008 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II), *OJ L* 299, 8.11.2008, pp. 1-8.

- Council Regulation (EC) No 1683/95 of 29 May 1995 laying down a uniform format for visas, *OJ L* 164, 14.7.1995, pp. 1-4.

- Council Regulation (EC) No 1968/2006 of 21 December 2006 concerning Community financial contributions to the International Fund for Ireland, *OJ* 2006, L 409, p. 8.

- Council Regulation (EC) No 1988/2006 of 21 December 2006 amending Regulation (EC) No 2424/2001 on the development of the second generation Schengen Information System (SIS II), *OJ L* 411, 30.12.2006, pp. 1-5.

- Council Regulation (EC) No 2201/2003 of 27 November 2003 concerning jurisdiction and the recognition and enforcement of judgments in matrimonial matters and the matters of parental responsibility, repealing Regulation (EC) No 1347/2000, *OJ L* 338, 23.12.2003, pp. 1-29.

- Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, *OJ L* 385, 29.12.2004, pp. 1-6.

- Council Regulation (EC) No 2424/2001 of 6 December 2001 on the development of the second generation Schengen Information System (SIS II), *OJ L* 328, 13.12.2001, pp. 4-6.

- Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, *OJ L* 316, 15.12.2000, pp. 1-10.

- Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, *OJ L* 50, 25.2.2003, pp. 1-10.

- Council Regulation (EC) No 380/2008 of 18 April 2008 amending Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals, *OJ L* 115, 29.4.2008, pp. 1-7.

- Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, *OJ L* 12, 16.1.2001, pp. 1-23.

- Council Regulation (EC) No 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, *OJ L* 162, 30.4.2004, pp. 29-31.

- Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), *OJ L* 283, 31.10.2017, pp. 1-7.

- Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing

Committee on the evaluation and implementation of Schengen, *OJ L* 295, 6.11.2013, pp. 27-37.

- Council Regulation (EU) No 1272/2012 of 20 December 2012 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II) (recast), *OJ L* 359, 29.12.2012, pp. 21-31.

- Council Regulation (EU) No 1273/2012 of 20 December 2012 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II) (recast), *OJ L* 359, 29.12.2012, pp. 32-44.

- Decision 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC Text with EEA relevance, *OJ L* 293, 5.11.2013, pp. 1-15.

- Decision 2002/463/EC adopting an action programme for administrative cooperation in the fields of external borders, visas, asylum and immigration, *OJ L* 371, 18.12.2004, pp. 48-49.

- Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on the interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC), *OJ L* 144, 30.4.2004, pp. 64-73.

- Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism, Text with EEA relevance, *OJ L* 347, 20.12.2013, pp. 924-947.

- Decision of the Council of the European Union of 5 December 2011 on the admission of the Republic of Croatia to the European Union, *OJ L* 112, 24.4.2012, pp. 6-110.

- Directive (EU) 2015/413 of the European Parliament and of the Council of 11 March 2015 facilitating cross-border exchange of information on road-safety-related traffic offences, *OJ L* 68, 13.3.2015, pp. 9-25.

- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L* 119, 4.5.2016, pp. 89-131.

- Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of Passenger Name Record (PNR) data for the prevention, detection,

investigation and prosecution of terrorist offences and serious crime, *OJ* EU L 119, 4.5.2016, pp. 132-149.

- Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law, *OJ* L 198, 28.7.2017, pp. 29-41.

- Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, *OJ* L 88, 31.3.2017, pp. 6-21 – confront Article 12.

- Directive (EU) 2017/853 of the European Parliament and of the Council of 17 May 2017 amending Council Directive 91/477/EEC on control of the acquisition and possession of weapons (Text with EEA relevance), *OJ* L 137, 24.5.2017, pp. 22-39.

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, *OJ* L 13, 19.1.2000, pp. 12-20.

- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *OJ* L 178, 17.7.2000, pp. 1-16.

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *OJ* L 201, 31.7.2002, pp. 37-47.

- Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation (market abuse), *OJ* L 96, 12.4.2003, pp. 16-25.

- Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications (Text with EEA relevance), *OJ* L 255, 30.9.2005, pp. 22-142.

- Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, *OJ* L 376, 27.12.2006, pp. 36-68.

- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ* L 105, 13.4.2006, pp. 54-63.

- Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals, *OJ L* 348, 24.12.2008, pp. 98-107.

- Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, *OJ L* 88, 4.4.2011, pp. 45-65.

- Directive 2011/82/EU of the European Parliament and of the Council of 25 October 2011 facilitating the cross-border exchange of information on road safety related traffic offences, *OJ L* 288, 5.11.2011, pp. 1-15.

- Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European protection order, *OJ L* 338, 21.12.2011, pp. 2-18.

- Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection, *OJ L* 180, 29.6.2013, pp. 60-95.

- Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *OJ L* 130, 1.5.2014, pp. 1-36.

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ L* 281, 23.11.1995, pp. 31-50.

- Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, *OJ L* 24, 30.1.1998, pp. 1-8.

- European Parliament resolution of 11 December 2018 on the full application of the provisions of the Schengen acquis in Bulgaria and Romania: abolition of checks at internal land, sea and air borders (2018/2092(INI)), *OJ C* 388, 13.11.2020, pp. 18-21.

- Framework Agreement on Partnership and Cooperation between the European Union and its Member States, of the one part, and the Republic of the Philippines, of the other part, *OJ L* 134, 24.5.2012, PE/33/2019/REV/1, *OJ L* 295, 14.11.2019, pp. 1-131.

- Joint Action 98/700/JHA of 3 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union concerning the setting up of a European Image Archiving System (FADO), *OJ L* 333, 9.12.1998, pp. 4-7.

- Protocol between the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the

Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a member State or in Switzerland, *OJ L* 160, 18.6.2011, p. 39.

- Protocol integrating the Schengen acquis into the framework of the European Union, *OJ C* 340, 10.11.1997, p. 93.

- Protocol No 36 on transitional provisions, *OJ C* 115, 9.5.2008, pp. 322-326.

- Recommendation for a Council Decision authorising the opening of negotiations for a cooperation agreement between the European Union and the International Criminal Police Organisation (ICPO- INTERPOL), COM(2021) 177 final, Brussels, 14.4.2021.

- Regulation (EC) 863/2007 of the European Parliament and of the Council of 11 July 2007 establishing a mechanism for the creation of Rapid border intervention teams and amending Council Regulation (EC) 2007/2004 as regards that mechanism and regulating the tasks and powers of guest officers, *OJ L* 199, 31.7.2007, pp. 30-39.

- Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, *OJ L* 145, 31.5.2001, pp. 43-48.

- Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates, *OJ L* 381, 28.12.2006, pp. 1-3.

- Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), *OJ L* 381, 28.12.2006, p. 4-23.

- Regulation (EC) No 390/2009 of the European Parliament and of the Council of 23 April 2009 amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications, *OJ L* 131, 28.5.2009, pp. 1-10.

- Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, *OJ L* 8, 12.1.2001, pp. 1-2.

- Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code), *OJ L* 105, 13.4.2006, pp. 1-32.

- Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), *OJ L* 218, 13.8.2008, pp. 60-81.

- Regulation (EC) No 81/2009 of the European Parliament and of the Council of 14 January 2009 amending Regulation (EC) No 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Borders Code, *OJ L* 35, 4.2.2009, pp. 56-58.

- Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code), *OJ L* 243, 15.9.2009, pp. 1-58.

- Regulation (EEC) No 1408/71 of the Council of 14 June 1971 on the application of social security schemes to employed persons and their families moving within the Community, *OJ L* 149, 5.7.1971, pp. 2-50.

- Regulation (EEC) No 574/72 of the Council of 21 March 1972 fixing the procedure for implementing Regulation (EEC) No 1408/71 on the application of social security schemes to employed persons and their families moving within the Community, *OJ L* 74, 27.3.1972, pp. 1-83.

- Regulation (EU) 1168/2011 of the European Parliament and of the Council of 25 October 2011 amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, *OJ L* 304, 22.11.2011, pp. 1-17.

- Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC, *OJ L* 251, 16.9.2016, pp. 1-76.

- Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), *OJ L* 77, 23.3.2016, pp. 1-52.

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), *OJ L* 119, 4.5.2016, pp. 1-88.

- Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, *OJ L* 135, 24.5.2016, pp. 53-114.

- Regulation (EU) 2017/1370 of the European Parliament and of the Council of 4 July 2017 amending Council Regulation (EC) No 1683/95 laying down a uniform format for visas, *OJ L* 198, 28.7.2017, pp. 24-28.

- Regulation (EU) 2017/2225 of the European Parliament and of the Council of 30 November 2017 amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System, *OJ L* 327, 9.12.2017, pp. 1-19.

- Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, *OJ L* 327, 9.12.2017, pp. 20-82.

- Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders, *OJ L* 74, 18.3.2017, pp. 1-7.

- Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, PE/21/2018/REV/1, *OJ L* 236, 19.9.2018, pp. 1-71.

- Regulation (EU) 2018/1241 of the European Parliament and of the Council of 12 September 2018 amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS), *OJ L* 236, 19.9.2018, pp. 72-73.

- Regulation (EU) 2018/1718 of the European Parliament and of the Council of 14 November 2018 amending Regulation (EC) No 726/2004 as regards the location of the seat of the European Medicines Agency Text with EEA relevance, PE/40/2018/REV/1, *OJ L* 291, 16.11.2018, pp. 3-4.

- Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures

and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (Text with EEA relevance) PE/41/2018/REV/2, *OJ L* 295, 21.11.2018, pp. 1-38.

- Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance), PE/31/2018/REV/1, *OJ L* 295, 21.11.2018, pp. 39-98.

- Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011, PE/29/2018/REV/1, *OJ L* 295, 21.11.2018, pp. 99-137.

- Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, PE/37/2018/REV/1, *OJ L* 295, 21.11.2018, pp. 138-183.

- Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 PE/35/2018/REV/1, *OJ L* 312, 7.12.2018, pp. 14-55.

- Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU PE/36/2018/REV/1, *OJ L* 312, 7.12.2018, pp. 56-106.

- Regulation (EU) 2019/1155 of the European Parliament and of the Council of 20 June 2019 amending Regulation (EC) No 810/2009 establishing a Community Code on Visas (Visa Code), PE/29/2019/REV/1, *OJ L* 188, 12.7.2019, pp. 25-54.

- Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624, *OJ L* 295, 14.11.2019, pp. 1-131.

- Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, PE/88/2018/REV/1, *OJ L* 135, 22.5.2019, pp. 1-26.

- Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, PE/30/2019/REV/1, *OJ L* 135, 22.5.2019, pp. 27-84.

- Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, PE/31/2019/REV/1, *OJ L* 135, 22.5.2019, pp. 85-135.

- Regulation (EU) 2020/493 of the European Parliament and of the Council of 30 March 2020 on the False and Authentic Documents Online (FADO) system and repealing Council Joint Action 98/700/JHA, PE/97/2019/REV/1, *OJ L* 107, 6.4.2020, pp. 1-8.

- Regulation (EU) 2021/1133 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EU) No 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 and (EU) 2019/818 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the Visa Information System, PE/45/2021/INIT, *OJ L* 248, 13.7.2021, pp. 1-10.

- Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System, *OJ L* 248, 13.7.2021, pp. 11-87.

- Regulation (EU) 2021/1151 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EU) 2019/816 and (EU) 2019/818 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the

European Travel Information and Authorisation System, PE/16/2021/REV/1, *OJ L* 249, 14.7.2021, pp. 7-14.

- Regulation (EU) 2021/1152 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No. 767/2008, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861 and (EU) 2019/817 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the European Travel Information and Authorisation System, PE/17/2021/REV/1, *OJ L* 249, 14.7.2021, pp. 15-37.

- Regulation (EU) 2021/2303 of the European Parliament and of the Council of 15 December 2021 on the European Union Agency for Asylum and repealing Regulation (EU) No 439/2010, PE/61/2021/REV/1, *OJ L* 468, 30.12.2021, pp. 1-54.

- Regulation (EU) 439/2010 of the European Parliament and of the Council of 19 May 2010 establishing a European Asylum Support Office, *OJ L* 132, 29.5.2010, pp. 11-28.

- Regulation (EU) 493/2011 of the European Parliament and of the Council of 5 April 2011 amending Council Regulation (EC) No 377/2004 on the creation of an immigration liaison officers network, *OJ L* 141, 27.5.2011, pp. 13-16.

- Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, *OJ L* 286, 1.11.2011, pp. 1-17.

- Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (ESMA), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC, *OJ L* 331, 15.12.2010, pp. 84-119.

- Regulation (EU) No 236/2012 of the European Parliament and of the Council of 14 March 2012 on short selling and certain aspects of credit default swaps Text with EEA relevance, *OJ L* 86, 24.3.2012, pp. 1-2.

- Regulation (EU) No 542/2010 of 3 June 2010 amending Decision 2008/839/JHA on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II), *OJ L* 155, 22.6.2010, pp. 23-26.

- Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC Text with EEA relevance, *OJ L* 173, 12.6.2014, pp. 1-61.

- Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, *OJ L 180*, 29.6.2013, pp. 1-30.

- Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person, *OJ L 180*, 29.6.2013, pp. 31-59.

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, *OJ L 257*, 28.8.2014, pp. 73-114.

- Status Agreement between the European Union and the Republic of Serbia on actions carried out by the European Border and Coast Guard Agency in the Republic of Serbia, *OJ L 202*, 25.6.2020.

- Treaty establishing a Constitution for Europe, Protocols and Annexes, FINAL ACT, *OJ C 310*, 16.12.2004, pp. 1-474.

- Treaty establishing the European Community (Amsterdam consolidated version), *OJ C 340*, 10.11.1997, pp. 173-306.

- Treaty establishing the European Community (Consolidated version 2002), *OJ C 325*, 24.12.2002, pp. 33-184.

- Treaty establishing the European Economic Community signed in Rome on 25 March 1957, entered into force on 1 January 1958.

- Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, *OJ C 306*, 17.12.2007, pp. 1-271.

- Treaty of Nice amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, *OJ C 80*, 10.3.2001, pp. 1-87.

- Treaty of the Treaty on the European Coal and Steel Community signed in Paris on 18 April 1951, entered into force on 23 July 1952.

- Treaty on European Union (consolidated version 1997), *OJ C* 340, 10.11.1997, pp. 145-17.

- Treaty on European Union, *OJ C* 191, 29.7.1992, pp. 1-112.

- Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union - Council Declaration on Article 10(9) - Declaration by the United Kingdom on Article 20, *OJ C* 197, 12.7.2000, pp. 3-23.

- Treaty on European Union, on the establishment of a European Police Office (Europol Convention), *OJ C* 316, 27.11.1995, pp. 1-32.

National Law

- Acuerdo entre el Reino de España y el Reino de Marruecos relativo a la circulación de personas, el tránsito y la readmisión de extranjeros entrados ilegalmente, hecho en Madrid el 13 de febrero de 1992, *Boletín Oficial del Estado* No. 299, 13.12.2012, p. 85068.

- Constitución Española, *Boletín Oficial del Estado* No. 311, 29.12.1978.

- Costituzione della Repubblica Italiana, *Gazzetta Ufficiale* No. 298, 27.12.1947.

- Decreto Legislativo 30 giugno 2003, No. 196, Codice in materia di protezione dei dati personali, ((recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) No. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE)), *Gazzetta Ufficiale* No. 174, 29.7.2003.

- Hessische Datenschutzgesetz vom 7. oktober 1970 GVBl. II 300-10, Gesetz-und Verordnungsblatt für das Land Hessen, Part I, No. 41, 12.10.1970.

- Legge 31 dicembre 1996, No. 675, Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, *Gazzetta Ufficiale* No. 5, 08.01.1997.

- Ley 25/2014, de 27 de noviembre, de Tratados y otros Acuerdos Internacionales, *Boletín Oficial del Estado* No. 288, 28.11.2014.

- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, *Boletín Oficial del Estado* No. 281, 24.11.1995.

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, *Boletín Oficial del Estado* No. 298, 14.12.1999.

- Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), *Boletín Oficial del Estado* No. 262, 31.10.1992.

- Loi No. 78–17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés, modifiée en dernier lieu par loi No. 2014-344 du 17 mars 2014, *Journal Officiel de la République Française*, 18.03.2014.

- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Public Law 107–56 — 26.10.2001, available at www.congress.gov.

Others

- Constitution of the ICPO-INTERPOL, adopted by the General Assembly at its 25 session, Vienna, 1956.

- Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, signed in the Netherlands, 18 March 1970, entered into force on 7 October 1972.

- Decision of the Executive Committee of 28 April 1999 on liaison officers, SCH/Com-ex (99) 7 rev. 2, *OJ L* 239, 22.09.2000.

- Decision of the Executive Committee on *a catch-all clause to cover the whole technical Schengen acquis*, SCH/Com-ex (98) 29 rev, Brussels, 23.06.1998.

- EEA joint committee, *Decision amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol No. 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022]*, No. 154/2018, 6 July 2018.

- ICRC, *Statutes of the International Committee of the Red Cross*, adopted in Geneva on 21 December 2017, entered into force on 1 January 2018.

- Interpol’s Rules on *the Processing of Data*, adopted by the General Assembly in 2011, entered into force in July 2012.

- Interpol’s Rules on *the Processing of Data*, No. III/IRPD/GA/2011, 1 April 2019, available.

- ISO/IEC 2382-37:2017, Information technology — Vocabulary —, 2017.

Jurisprudence

International Court of Justice

- International Court of Justice (ICJ), Advisory Opinion, *Reparation for Injuries Suffered in the Service of the United Nations*, 1949, ICJ Rep. 174.

- International Court of Justice (ICJ), Judgment, *La Grand (Germany v USA)*, 2001, ICJ Rep. 466.

European Court of Human Rights

- *Amann v Switzerland*, No. 27798/95, 16 February 2000, CE:ECHR:2000:0216JUD002779895.

- *Behrami and Behrami v France, and Saramati v France, Germany and Norway* [GC], No. 71412/01 and No. 78166/01, 2 May 2007, CE:ECHR:2007:0502DEC007141201.

- *Big Brother Watch and Others v the United Kingdom* [GC], Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021, CE:ECHR:2021:0525JUD005817013.

- *Bosphorus hava yollari turizm ve ticaret anonim şirketi v Ireland*, No. 45036/98, 30 June 2005, CE:ECHR:2005:0630JUD004503698.

- *Centrum för rättvisa v Sweden* [GC], No. 35252/08, 25 May 2021, CE:ECHR:2021:0525JUD003525208.

- *Fredl v Austria*, No. 15225/89, 19 May 1994, ECHR:1994:0519REP001522589.

- *Gaskin v the United Kingdom* [GC], No. 10454/83, 7 July 1989, CE:ECHR:1989:0707JUD001045483.

- *Halford v United Kingdom*, No. 20605/92, 25 June 1997, CE:ECHR:1997:0625JUD002060592.

- *Jivan v Romania*, No. 62250/19, 8 February 2022, CE:ECHR:2022:0208JUD006225019.

- *Kennedy v the United Kingdom*, No. 26839/05, 18 August 2010, CE:ECHR:2010:0518JUD002683905.

- *Khelili v Switzerland*, No. 16188/07, 8 March 2012, CE:ECHR:2011:1018JUD001618807.

- *Klass and Others v Germany*, No. 5029/71, 6 September 1978, CE:ECHR:1978:0906JUD000502971.

- *Leander v Sweden*, No. 9248/81, 26 March 1987, CE:ECHR:1987:0326JUD000924881.

- *Liberty and Others v the United Kingdom*, No. 58243/00, 1 October 2008, CE:ECHR:2008:0701JUD005824300.

- *Malone v the United Kingdom*, No. 8691/79, 2 August 1984, CE:ECHR:1984:0802JUD00086917.

- *Niemietz v Germany*, No. 13710/88, 16 December 1992, CE:ECHR:1992:1216JUD001371088.

- *P.G. and J.H. v. the United Kingdom*, No. 44787/98, 25 December 2001, CE:ECHR:2001:0925JUD004478798.

- *Roman Zakharov v Russia*, No. 47143/06, 4 December 2015, CE:ECHR:2015:1204JUD004714306.

- *Rotaru v Romania* [GC], No. 28341/95, 4 May 2000, CE:ECHR:2000:0504JUD002834195.

- *S. and Marper v the United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008, CE:ECHR:2008:1204JUD003056204.

- *Weber and Saravia v Germany*, No. 54934/00, 26 June 2006, CE:ECHR:2006:0629DEC005493400.

Court of Justice of the European Union

- C-101/01, *Bodil Lindqvist v Åklagarkammaren i Jönköping*, 19 September 2002, EU:C:2002:513.

- C-104/81, *Hauptzollamt Mainz v C.A. Kupferberg & Cie KG a.A.*, 26 October 1982, EU:C:1982:362.

- C-11/70, *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel*, 17 December 1970, EU:C:1970:114.

- C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González*, 13 May 2014, EU:C:2014:317.

- C-136/17, *GC, AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL)*, 24 September 2019, EU:C:2019:773.

- C-149/96, *Portuguese Republic v Council of the European Union*, 23 November 1999, EU:C:1999:574.

- C-160/03, *Kingdom of Spain v Eurojust*, 15 March 2005, EU:C:2005:168.

- C-166/077, *European Parliament v Council*, 3 September 2009, EU:C:2009:499.

- C-170/96, *Commission v Council*, 20 May 2008, EU:C:2008:288.

- C-176/03, *Commission of the European Communities v Council of the European Union*, 13 September 2005, EU:C:2005:542.

- C-178/03, *Commission v European Parliament and Council*, 10 January 2006, EU:C:2006:4.

- C-18/19, *WM v Stadt Frankfurt am Main*, 2 July 2020, EU:C:2020:511.
- C-192/15, *Rease and Wullems*, of 9 December 2015, EU:C:2015:861.
- C-193/19, *A v Migrationsverket*, 4 March 2021, EU:C:2021:168.
- C-201/14, *Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF)*, 1 October 2015, EU:C:2015:638.
- C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen, and Secretary of State for the Home Department v Tom Watson, Peter Brice, and Geoffrey Lewis*, 21 December 2016, EU:C:2016:970.
- C-207/16, *Ministerio Fiscal*, 2 October 2018, EU:C:2018:788.
- C-209/97, *Commission of the European Communities v Council of the European Union*, 18 November 1999, EU:C:1999:559.
- C-21 to 24/72, *International Fruit Company NV and others v Produktschap voor Groenten en Fruit*, 12 December 1972, EU:C:1972:115.
- C-211/01, *Commission of the European Communities v Council*, 11 September 2003, EU:C:2003:452.
- C-22/70, *Commission of the European Communities v Council of the European Communities*, 31 March 1971, EU:C:1971:32.
- C-225/12, *Demir*, 7 November 2013, EU:C:2013:725.
- C-230/14, *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1 October 2015, EU:C:2015:639.
- C-240/09, *Lesoochránárske zoskupenie VLK v. Ministerstvo životného prostredia Slovenskej republiky*, of 8 March 2011, EU:C:2011:125.
- C-245/19 and C-246/19, *État luxembourgeois v B, and État luxembourgeois v B, C, D, F.C.*, 6 October 2020, EU:C:2020:795.
- C-25/17, *Tietosuojaalvautettu*, 10 July 2018, EU:C:2018:551.
- C-26/62, *Van Gend en Loos v Administratie der Belastingen*, 5 February 1963, EU:C:1963:1.
- C-260/89, *ERT v DEP*, 18 June 1991, EU:C:1991:254.
- C-263/14, *Parliament v Council (Tanzania)*, EU:C:2016:435.
- C-265/03, *Simutenkov v Ministerio de Educación y Cultura and Others*, 12 April 2005, EU:C:2005:213.
- C-266/03, *Commission of the European Communities v Grand Duchy of Luxemburg*, 2 June 2005, EU:C:2005:341.

- C-268/94, *Portuguese Republic v Council of the European Union*, 3 December 1996, EU:C:1996:461.
- C-270/12, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*, 22 January 2014, EU:C:2014:18.
- C-271/94, *European Parliament v Council of the European Union*, 26 March 1996, EU:C:1996:133.
- C-272/19, *VQ v Land Hessen*, 9 July 2020, EU:C:2020:535.
- C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, EU:C:2008:54, 29 January 2008.
- C-281, 283, 284, 285 and 287/85, *Germany and Others v Commission*, 9 July 1987, EU:C:1987:351.
- C-29/69, *Stauder v Stadt Ulm*, 24 June 1969 EU:C:1969:27.
- C-291/12, *Michael Schwarz v Stadt Bochum*, 17 October 2013, EU:C:2013:670.
- C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014, EU:C:2014:238.
- C-3, 4 and 6/76, *Cornelis Kramer and others*, 14 July 1976, EU:C:1976:114.
- C-300/89, *Commission of the European Communities v Council of the European Communities*, 11 June 1991, EU:C:1991:244.
- C-301/06, *Ireland v European Parliament and Council of the European Union*, 10 February 2009, EU:C:2009:68.
- C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd, and Maximillian Schrems*, 16 July 2020, EU:C:2020:559.
- C-316/91, *European Parliament v Council of the European Union*, 2 March 1994, EU:C:1994:76.
- C-317/04 and C-318/04, *Parliament v Council of the European Union and Commission of the European Communities*, EU:C:2006:346.
- C-327/91, *French Republic v Commission of the European Communities*, 9 August 1994, EU:C:1994:305.
- C-337/95, *Parfums Christian Dior SA and Parfums Christian Dior BV and Evora BV*, 4 November 1997, EU:C:1997:517.
- C-338/01, *Commission of the European Communities v Council of the European Union*, 26 January 2005, EU:C:2004:253.
- C-358/16, *UBS Europe and Others*, 13 September 2018, EU:C:2018:715.

- C-36/75, *Roland Rutili v Ministre de l'intérieur*, 28 October 1975, EU:C:1975:137.
- C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015, EU:C:2015:650, and C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd, and Maximillian Schrems*, 16 July 2020, EU:C:2020:559.
- C-368/20 and C-369/20, *NW v Landespolizeidirektion Steiermark (C-368/20), Bezirkshauptmannschaft Leibnitz (C-369/20)*, 26 April 2022, EU:C:2022:298.
- C-376/98, *Federal Republic of Germany v European Parliament, and Council of the European Union*, 5 October 2000, EU:C:2000:544.
- C-378/97, *Florus Ariël Wijsenbeek*, 21 September 1999, EU:C:1999:439.
- C-4/73, *Nold KG v Commission*, 14 May 1974, EU:C:1974:51.
- C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, 29 July 2019, EU:C:2019:629.
- C-402/05 P and C-415/05 P, *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities*, 3 September 2008, EU:C:2008:461.
- C-411/06, *Sogelma – Società generale lavori manutenzioni appalti Srl v European Agency for Reconstruction (EAR)*, 8 October 2008, EU:T:2008:419.
- C-425/13, *Commission v Council (Australia emissions trading system)*, EU:C:2015:483.
- C-427/12, *European Commission v European Parliament, Council of the European Union*, 18 March 2014, EU:C:2014:170.
- C-431/05, *Merck Genéricos – Produtos Farmacêuticos Lda v Merck & Co. Inc.*, 11 September 2007, EU:C:2007:496.
- C-431/11, *United Kingdom of Great Britain and Northern Ireland v Council of the European Union*, 26 September 2013, EU:C:2013:589.
- C-434/16, *Peter Nowak v Data Protection Commissioner*, 20 December 2017, EU:C:2017:994.
- C-446/12 to C-449/12, *W.P. Willems v Burgemeester van Nuth and H.J. Kooistra v Burgemeester van Skarsterlân and M. Roest v Burgemeester van Amsterdam and L.J.A. van Luijk v Burgemeester van Den Haag*, 16 April 2015, EU:C:2015:238.
- C-46/87 and C-227/88, *Hoechst v Commission*, of 21 September 1989, EU:C:1989:337.
- C-465/00, C-138/01 and C-139/01, *Rundfunk*, 20 May 2003, EU:C:2003:294.
- C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECMD) v Administración del Estado*, 24 November 2011, EU:C:2011:777.

- C-469/93, *Amministrazione delle Finanze dello Stato v. Chiquita Italia*, 12 December 1995, EU:C:1995:435.
- C-471/98, *Commission of the European Communities v Kingdom of Belgium*, 5 November 2002, EU:C:2002:628.
- C-473/12, *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert, Immo 9 SPRL, Grégory Francotte*, 7 November 2013, EU:C:2013:715.
- C-482/08, *United Kingdom of Great Britain and Northern Ireland v Council of the European Union*, 16 October 2010, EU:C:2010:631.
- C-511/18, C-512/18 and C-520/18, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, v Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées*, 6 October 2020, EU:C:2020:791.
- C-518/07, *European Commission v Federal Republic of Germany*, 9 March 2010, EU:C:2010:125.
- C-524/06, *Heinz Huber v Bundesrepublik Deutschland*, 16 December 2008, ECLI:EU:C:2008:724.
- C-53/96, *Hermès International (a partnership limited by shares) and FHT Marketing Choice BV*, 16 June 1998, EU:C:1998:292.
- C-540/13, *European Parliament v Council of the European Union*, 16 April 2015, EU:C:2015:224.
- C-543/09, *Deutsche Telekom AG v Bundesrepublik Deutschland*, 5 May 2011, EU:C:2011:279.
- C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, 19 October 2016, EU:C:2016:779.
- C-584/10 P, C-593/10 P and C-595/10 P, *European Commission and Others v Yassin Abdullah Kadi*, 18 July 2013, EU:C:2013:518
- C-601/15 PPU, *J. N. v Staatssecretaris voor Veiligheid en Justitie*, 15 February 2016, EU:C:2016:84.
- C-61/19, *Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*, 11 November 2020, EU:C:2020:901.
- C-614/10, *European Commission v Austria*, 16 October 2012, EU:C:2012:.
- C-617/10, *Åklagaren v Hans Åkerberg Fransson*, 26 February 2013, EU:C:2013:105.
- C-620/19, *Land Nordrhein-Westfalen v D.-H.T.*, 10 December 2020, EU:C:2020:1011.
- C-623/17, *Privacy International*, 6 October 2020, EU:C:2020:790.

- C-656/11, *United Kingdom of Great Britain and Northern Ireland v Council of the European Union*, 27 February 2014, EU:C:2014:97
- C-658/11, *European Parliament v Council of the European Union*, 24 June 2014, EU:C:2014:2025.
- C-658/19, *European Commission v Kingdom of Spain*, 25 February 2021, EU:C:2021:138.
- C-66/13, *Green Network Spa v Autorità per l'energia elettrica e il gas*, 26 November 2014, EU:C:2014:2399.
- C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH*, 1 October 2019, EU:C:2019:801.
- C-73/14, *Council of the European Union v European Commission*, EU:C:2015:663.
- C-73/16, *Peter Puškár v Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy*, 27 September 2017, EU:C:2017:725.
- C-77/05, *United Kingdom of Great Britain and Northern Ireland v Council of the European Union*, 18 December 2007, EU:C:2007:803,.
- C-8/55, *Fédération Charbonnière de Belgique v High Authority of the European Coal and Steel Community*, 16 July 1956, EU:C:1956:7.
- C-89/18, *A v Udlændingeog Integrationsministeriet*, 10 July 2019, EU:C:2019:580.
- C-9/56, *Meroni & Co., Industrie Metallurgiche, SpA v High Authority of the European Coal and Steel Community*, 13 June 1958, EU:C:1958:7.
- C-92/09 and C-93/09, *Volker und Markus Schecke GbR, Hartmut Eifert v Land Hessen*, 9 November 2010, EU:C:2010:662.
- C-98/80, *Giuseppe Romano and Institut National d'Assurance Maladie-Invalidité*, 14 May 1981, EU:C:1981:104.
- C-133/06, *European Parliament v Council*, 6 May 2008, EU:C:2008:257.
- C-140/20, *G.D. v Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General*, 5 April 2022, EU:C:2022:258.
- C-746/18, *H. K., Prokuratuur*, 2 March 2021, EU:C:2021:152.
- C-114/12, *European Parliament v Council of the European Union*, 4 September 2014, EU:C:2014:2151.
- C-130/10, *European Parliament v Council of the European Union*, 19 July 2012, EU:C:2012:472.

- C-141/12 and C-372/12, *YS v Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v M. S.*, 17 July 2014, EU:C:2014:2081.
- C-217/04, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*, 2 May 2006, EU:C:2006:279.
- C-270/12, *United Kingdom of Great Britain and Northern Ireland, represented by A. Robinson, acting as Agent, J. Stratford QC and A. Henshaw, Barrister, applicant, v European Parliament, represented by A. Neergaard, R. Van de Westelaken, D. Gauci and A. Gros-Tchorbadjiyska, acting as Agents, Council of the European Union*, 22 January 2014, EU:C:2014:18.
- C-278/12 PPU, *Atiqullah Adil v Minister voor Immigratie, Integratie en Asiel*, 19 July 2012, EU:C:2012:508.
- C-363/14, *European Parliament, represented by F. Drexler, A. Caiola and M. Pencheva, acting as Agents, with an address for service in Luxembourg, applicant, v Council of the European Union*, 10 September 2015, EU:C:2015:579.
- C-377/12, *European Commission v Council of the European Union*, 11 June 2014, EU:C:2014:1903.
- C-38/06, *European Commission v Portugal*, 4 March 2010, EU:C:2010:108.
- C-396/11, *Ciprian Vasile Radu*, 2 January 2013, EU:C:2013:39.
- C-399/11, *Stefano Melloni v Ministerio Fiscal*, 26 February 2013, EU:C:2013:107.
- C-43/12, *European Commission v European Parliament and the Council*, 6 May 2014, EU:C:2014:298.
- C-439/19, *B and Latvijas Republikas Saeima*, 22 June 2021, EU:C:2021:504.
- C-461/05, *European Commission v Denmark*, December 2009, EU:C:2009:783.
- C-482/17, *Czech Republic, v European Parliament and Council of the European Union*, 3 December 2019, paras. 159-171, EU:C:2019:1035.
- C-505/1, *WS v Bundesrepublik Deutschland*, 12 May 2021, EU:C:2021:376.
- C-528/15, *Al Chodor*, 15 March 2017, EU:C:2017:213.
- C-645/19, *Facebook Belgium BVBA v Gegevensbeschermingsautoriteit*, 15 June 2021, EU:C:2021:483.
- C-660/13, *Council of the European Union v European Commission*, 28 July 2016, EU:C:2016:616.
- C-715/17, C-718/17 and C-719/17, *European Commission v Republic of Poland*, 2 April 2020, EU:C:2020:257.
- *Opinion I/13*, 14 October 2014, EU:C:2014:2303.

- *Opinion 1/15*, 26 July 2017, EU:C:2017:592.
- *Opinion 1/76*, 26 April 1977, EU:C:1977:63.
- *Opinion 1/92*, 10 April 1992, EU:C:1992:189.
- *Opinion 1/94*, 15 November 1994, EU:C:1994:384.
- *Opinion 2/00*, 6 December 2001, EU:C:2001:664.
- *Opinion 2/13*, 18 December 2014, EU:C:2014:2454.
- *Opinion 2/15*, 16 May 2017, EU:C:2017:376
- *Opinion 2/91*, 19 March 1993, EU:C:1993:106.
- *Opinion 2/94*, 28 March 1996, EU:C:1996:140.
- Opinion Advocate General De La Tour, C-193/19, *A v Migrationsverket*, 16 July 2020, EU:C:2020:594.
- Opinion of Advocate General Bobek, C505/1, *WS v Bundesrepublik Deutschland*, 19 November 2020, EU:C:2020:939.
- Opinion of Advocate General Bobek, C-59/18 and C-182/18, *Italian Republic (C-59/18) Comune di Milano (C-182/18) v Council of the European Union*, 6 October 2021, EU:C:2021:812.
- Opinion of Advocate General Bobek, C-106/19 and C-232/19, *Italian Republic (C-106/19) Comune di Milano (C-232/19) v Council of the European Union*, 6 October 2021, EU:C:2021:816.
- Opinion of Advocate General Capotorti, C-155/80, *Procureur Général v. Arbelaiz-Emazebel*, 27 May 1981, EU:C:1981:123.
- Opinion of Advocate General Cruz Villalón, C-650/13, *Thierry Delvigne/Commune de Lesparre Médoc and Préfet de la Gironde*, 4 June 2015, ECLI:EU:C:2015:363.
- Opinion of Advocate General Fennelly, C-170/96, *Commission v Council*, 12 May 1998, EU:C:1998:219.
- Opinion of Advocate General Pitruzzella, C-817/19, *Ligue des droits humains v Conseil des ministres*, 27 January 2022, EU:C:2022:65.
- Opinion of Advocate General Jääskinen, C-270/12, *Digital reports (Court Reports - general), United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*, 12 September 2013, EU:C:2013:562.
- Opinion of Advocate General Kokott, C-263/14, *European Parliament v Council of the European Union*, EU:C:2015:729.

- Opinion of Advocate General Sánchez Bordona, C-793/19 and C-794/19, *Bundesrepublik Deutschland v SpaceNet AG (C-793/19) Telekom Deutschland GmbH (C-794/19)*, 18 November 2021, EU:C:2021:939.

- Opinion of Advocate General Sánchez Bordona, C-339/20 and C-397/20, *VD (C-339/20), SR (C-397/20)*, 18 November 2021, EU:C:2021:940.

- Opinion of Advocate General Tesauro, C-327/91, *French Republic v Commission of the European Communities*, 16 December 1993, EU:C:1993:941.

- Opinion of Advocate General Tizzano, C-465/00, *Neukomm and Lauremann v Österreichischer Rundfunk*, 14 November 2002, EU:C:2002:662.

- Opinion of Advocate General Van Gerven, C-137/92 P, *Commission of the European Communities v BASF AG, Limburgse Vinyl Maatschappij NV, DSM NV, DSM Kunststoffen BV, Hüls AG, Elf Atochem SA, Société Artésienne de Vinyle SA, Wacker Chemie GmbH, Enichem SpA, Hoechst AG, Imperial Chemical Industries plc, Shell International Chemical Company Ltd and Montedison SpA*, 29 June 2003, EU:C:1994:247.

- Opinion of Advocate General Yves Bot, C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 23 September 2015, EU:C:2015:627.

- T-115/13, *Gert-Jan Dennekamp v European Parliament*, 5 July 2015, EU:T:2015:497.

- T-85/09, *Kadi v Commission*, 30 September 2010

- T-526/10, *Inuit Tapiriit Kanatami, Nattivak Hunters and Trappers Association, Pangnirtung Hunters' and Trappers' Association, Jaypootie Moesesie, Allen Kooneeliusie, residing in Qikiqtarjuaq, Toomasie Newkingnak, David Kuptana, Karliin Ariak, Canadian Seal Marketing Group, Ta Ma Su Seal Products, Fur Institute of Canada, NuTan Furs, Inc., GC Rieber Skinn AS, Inuit Circumpolar Council Greenland (ICC-Greenland), Johannes Egede, Kalaallit Nunaanni Aalisartut Piniartullu Kattuffiat (KNAPK), William E. Scott & Son, Association des chasseurs de phoques des Îles-de-la-Madeleine, Hatem Yavuz Deri Sanayi iç Ve Diş Ticaret Ltd Şirketi, Northeast Coast Sealers' Co-Operative Society, Ltd, v European Commission*, 25 April 2013, EU:T:2013:215.

National Courts

- High Court of Justice, *The Queen (on application of Edward Bridges) - and - the Chief Constable of South Wales Police*, 4 September 2019, CO/4085/2018, available at www.judiciary.uk.

Other sources

United Nations

- General Comment No. 16 on Article 17 (Right to Privacy) of the Human Rights Committee of 8 April 1988, *The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*.
- Records of the meeting No. 54 of the General Assembly A/C.3/69/SR.54 of 25 November 2014.
- Report of the International Law Commission No. A/73/10 of 30 April-1 June and 2 July-10 August 2018, Seventieth session.
- Resolution of the General Assembly No. A/RES/428(V) of 14 December 1950, *Statute of the office of the United Nations high commissioner for refugees*.
- Resolution of the Human Rights Council No. A/HRC/28/16 of 26 March 2015, *The right to privacy in the digital age*.
- Resolution of the Human Rights Council No. A/HRC/28/39 of 19 December 2014, *Summary of the Human Rights Council panel discussion on the right to privacy in the digital age*.
- Resolution of the Human Rights Council No. A/HRC/39/29 of 3 August 2018, *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights*.
- Resolution of the Human Rights Council No. A/HRC/45/95 of 14 December 1990, *Guidelines for the regulation of computerized personal data files*.
- Resolution of the UN General Assembly No. A/RES/217/(III) of 10 December 1948, *Universal Declaration of Human Rights*.
- Resolution of the UN General Assembly No. A/RES/48/141 of 20 de December of 1993, *High Commissioner for the promotion and protection of all human rights*.
- Resolution of the UN General Assembly No. A/RES/56/83 of 28 January 2002, *Responsibility of States for internationally wrongful acts*.
- Resolution of the UN Human Rights Council No. A/HRC/37/62 of 25 October 2018, *Report of the Special Rapporteur on the right to privacy*.
- Resolution of the UN General Assembly No. A/RES/68/167 of 18 December 2013, *The right to privacy in the digital age*.
- Resolution of the UN General Assembly No. A/RES/71/199 of 19 December 2016, *The right to privacy in the digital age*.

- Resolution of the UN General Assembly No. A/RES/73/179 of 17 December 2018, *The right to privacy in the digital age*.
- Resolution of the UN General Assembly No. A/RES/75/176 of 16 December 2020, *The right to privacy in the digital age*.
- Resolution of the Human Rights Council No. A/HRC/RES/48/4 of 13 October 2021, *Right to privacy in the digital age*.
- Resolution No. A/RES/2450(XXIII) of 19 December 1968, *Human rights and scientific and technological developments*.
- United Nations HRI/GEN/Rev.5 of 26 April 2001, *Compilation of General Comments and General Recommendations Adopted by the Human Rights Treaty Bodies*.
- International Law Commission No. 10 (A/56/10) of 10 August 2001, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*.
- Resolution of the Human Rights Council No. A/HRC/38/7 of 5 July 2018, *Promotion, protection and enjoyment of human rights on the Internet*.
- Resolution of the Human Rights Council No. A/HRC/37/2 of 22 March 2018, *The right to privacy in the digital age*.
- Resolution of the Human Rights Council No. A/HRC/34/7 of 23 March 2017, *The right to privacy in the digital age*.
- Resolution of the Human Rights Council No. A/HRC/27/37 of 30 June 2014, *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*.
- Resolution of the Human Rights Council No. A/HRC/32/13 of 1 July 2016, *The promotion, protection and enjoyment of human rights on the Internet*.
- Resolution of the Human Rights Council No. A/HRC/48/31 of 13 September 2021, *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights*.
- Resolution of the Human Rights Council No. A/HRC/42/15 of 26 September 2019, *The right to privacy in the digital age*.
- Resolutions of the UN General Assembly No. A/RES/69/166 of 18 December 2014, *The right to privacy in the digital age*.
- Resolution, No. E/RES/2021/10 of 8 June 2021, *Socially just transition towards sustainable development: the role of digital technologies on social development and well-being of all*.

- Resolution, No. E/RES/2021/28 of 22 July 2021, *Assessment of the progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society*.

- Resolution, No. E/RES/2021/29 of 22 July 2021, *Science, technology and innovation for development*.

- Resolution, No. E/RES/2021/30 of 22 July 2021, *Open-source technologies for sustainable development*.

- UN General Assembly No. A/RES/73/151 of 17 December 2018, *Office of the United Nations High Commissioner for Refugees*.

- UN General Assembly No. A/RES/73/195 of 19 December 2018, *Global Compact for Safe, Orderly and Regular Migration*.

- UN General Secretary Resolution No. A/74/821 of 29 May 2020, *Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation*.

Council of Europe

- Committee of Ministers Recommendation R (87) 15 regulating *the use of personal data in the police sector*, Strasbourg, 17 September 1987.

- Committee on Legal Affairs and Human Rights, *Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (ETS No. 108), and its explanatory report*, Strasbourg, 15 November 2017.

- Council of Europe Recommendation of the Committee of Ministers on *the interoperability of information systems in the justice sector*, REC(2003)14, Strasbourg, 9 September 2003.

- Council of Europe, *Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Strasbourg, 10 October 2018.

- Council of Europe, *Non-members States of the Council of Europe: Five years validity of an invitation to sign and ratify or to accede to the Council of Europe's treatie*", Strasbourg, 16 February 2022.

- Decision of the Committee of Ministers of the session No. 128 on *Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Elsinore, 18 May 2018.

- Explanatory Report of the Council of Europe on *the Convention for the protection of individuals with regard to Automatic Processing of Personal Data*, Strasbourg, 21 January 1981.
- Recommendation of the Parliamentary Assembly of the Council of Europe No. 890 on *the protection of personal data*, Strasbourg, 1 February 1980.
- Recommendations of the Parliamentary Assembly of the Council of Europe No. 509 on *Human rights and modern scientific and technological developments*, Strasbourg, 31 January 1968.
- Report of the European Commission for Democracy through Law (“the Venice Commission”) on *the Democratic Oversight of Signals Intelligence Agencies*, Strasbourg, 20-21 March 2015.
- Report on *the first evaluation of Recommendation R (87) 15 regulating the use of personal data in the police sector*, Strasbourg, 1994.
- Report on *the second evaluation of Recommendation R (87) 15 regulating the use of personal data in the police sector*, Strasbourg, 1998.
- Report on *the third evaluation of Recommendation R (87) 15 regulating the use of personal data in the police sector*, Strasbourg, 2002.
- Resolution of the Committee of Ministers No. 73(22) on *the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*, Strasbourg, 26 September 1973.
- Resolution of the Committee of Ministers No. 74(29) on *the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*, Strasbourg, 20 September 1974.
- Resolution of the Parliamentary Assembly No. 721 on *data processing and the protection of human rights*, Strasbourg, 1 February 1980.
- Treaty Office of the Council of Europe, *Practical Guide to procedures applicable to the daily management of acts concerning the conventions of the Council of Europe*, Strasbourg, 2020.

European Union

Institutions

- Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(92) 422 final, Brussels, 15.10.1992.

- Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of Regulation (EU) XXX/XXX [Regulation on Asylum and Migration Management] and of Regulation (EU) XXX/XXX [Resettlement Regulation], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulations (EU) 2018/1240 and (EU) 2019/818, COM(2020) 614 final, Brussels, 23.9.2020.

- Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No. [...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No. 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version), COM(2012) 0254 final, Brussels, 4.5.2016.

- Commission Communication on the Digitalisation of justice in the European Union - A toolbox of opportunities, COM(2020) 710 final, Brussels, 2.12.2020.

- Commission Communication on the protection of individuals in relation to the processing of personal data in the community and information security, COM(90) 314 final, Brussels, 13.09.1990.

- Commission Decision of 17 June 2016 setting up the high-level expert group on information systems and interoperability C/2016/3780, OJ C 257, Brussels, 15.7.2016, pp. 3-6.

- Commission Decision on the Request by Ireland to accept Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of

Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), 11 December 2014, C(2014) 9310 final, *OJ L* 180, 29.6.2013, pp. 1-30.

- Commission Recommendation (EU) 2020/1364 of 23 September 2020 on legal pathways to protection in the EU: promoting resettlement, humanitarian admission and other complementary pathways, C(2020) 6467, *OJ L* 317, 1.10.2020, pp. 13-22.

- Commission Recommendation 81/679/EEC of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data, *OJ L* 246, 29.8.1981, p. 31.

- Commission Recommendation of 12.5.2017 on proportionate police checks and police cooperation in the Schengen area, C(2017) 3349 final, Brussels, 12.5.2017.

- Commission Regulation (EC, Euratom) No 2343/2002 of 23 December 2002 on the framework Financial Regulation for the bodies referred to in Article 185 of Council Regulation (EC, Euratom) No 1605/2002 on the Financial Regulation applicable to the general budget of the European Communities, *OJ L* 357, 31.12.2002, pp. 72-90.

- Commission Staff Working Document accompanying document to the Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice and Proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty, COM(2009) 293 final, Brussels, 24.06.2009.

- Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA, SWD(2018) 195 final, Brussels, 16.5.2018.

- Commission Staff Working Document impact assessment, Accompanying the document Proposal for a Regulation of the European Council on establishing a framework

for interoperability between eu information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 and Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between eu information systems (police and judicial cooperation, asylum and migration), SWD(2017) 0473 final, Strasbourg, 12.12.2017.

- Commission Staff Working Document Impact Assessment, Impact Assessment Report on the establishment of an EU Entry Exit System, SWD(2016) 115 final, Brussels, 6.4.2016.

- Commission Staff Working Document, Accompanying the document Report from the Commission to the European Parliament and the Council concerning the exchange through the European Criminal Records Information System (ECRIS) of information extracted from criminal records between the Member States, SWD(2020) 378 final, Brussels, 21.12.2020.

- Commission Staff Working Document, Analytical Supporting Document Accompanying the document Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless people (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011, SWD(2017) 248 final, Brussels, 29.6.2017, p. 6.

- Commission Staff Working Paper, First annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit, SEC(2004) 557, Brussels, 5.5.2004.

- Commission Staff Working Paper, Second annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit, SEC(2005) 839, 20.05.2005.

- Commission Staff Working Paper, Third annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit, SEC(2006), 21.11.2006.

- Common Position (EC) No 1/95 adopted by the Council on 20 February 1995 with a view to adopting Directive 95/. . /EC of the European Parliament and of the Council of . . . on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ C* 93, 13.4.1995, pp. 1-24.

- Communication by the Commission of the European Communities concerning a Community policy for data processing, Brussels, SEC(73) 4300, Brussels, 21.11.1973.

- Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries, COM(2010) 0492 final, Brussels, 21.9.2010.

- Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597 final, Brussels, 24.11.2005.

- Communication from the Commission to the Council, Community policy on data processing, SEC(73) 4300 final, Brussels, 21.11.1973.

- Communication from the Commission to the European Parliament and the Council, Stronger and Smarter Information Systems for Borders and Security, COM(2016) 205 final, Brussels, 6.04.2016.

- Communication from the Commission to the European Parliament and the Council - European agencies – The way forward, COM(2008) 135 final, Brussels, 11.3.2008.

- Communication from the Commission to the European Parliament and the Council, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, COM(2010) 673 final, Brussels, 22.11.2010.

- Communication from the Commission to the European Parliament and the Council, Towards a reform of the common European Asylum system and enhancing legal avenues to Europe, COM(2016) 197 final, Brussels, 6.4.2016.

- Communication from the Commission to the European Parliament and the Council - Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2007, COM(2009) 0013 final, Brussels, 26.1.2009.

- Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World, COM(2017) 7 final, Brussels, 10.1.2017.

- Communication from the Commission to the European Parliament and the Council, Overview of information management in the area of freedom, security and justice, COM(2010) 0385 final, Brussels, 20.7.2010.

- Communication from the Commission to the European Parliament and the Council - Consequences of the entry into force of the Treaty of Lisbon for ongoing interinstitutional decision-making procedures, COM(2009) 0665 final, Brussels, 2.12.2009.

- Communication from the Commission to the European Parliament and the Council, Way forward on aligning the former third pillar acquis with data protection rules, COM(2020) 262 final, Brussels, 24.6.2020.

- Communication from the Commission to the European Parliament and the Council, Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM), COM(2012) 0735 final, Brussels, 7.12.2012.

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions empty, 2030 Digital Compass: the European way for the Digital Decade, COM(2021) 118 final, Brussels, 9.3.2021.

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions Policy Plan on Asylum, COM(2008) 360 final, Brussels, 17.6.2008.

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, a European Agenda on Migration, COM(2015) 240 final, Brussels, 13.5.2015.

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Report on the evaluation and future development of the FRONTEX Agency, COM(2008) 67 final, Brussels, 13.02.2008.

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Better regulation: Joining forces to make better laws, COM(2021) 219 final, Brussels, 29.4.2021.

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Preparing the next steps in border management in the European Union, COM(2008) 0069 final, Brussels, 13.02.2008.

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2010) 171 final, Brussels, 20.4.2010.

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Safeguarding Privacy in a Connected World, A European Data Protection Framework for the 21st Century, COM(2012) 9 final, Brussels, 25.1.2012.

- Communication from the Commission, Better Regulation: Delivering better results for a stronger Union, COM(2016) 615 final, Brussels, 14.9.2016.

- Council of the EU - *Notification from Iceland*, 6750/20, Brussels, 11 March 2020.

- Council of the EU Secretariat's Note, *Framework for mutual collaboration and exchanging classified information between Europol and the General Secretariat of the Council*, 14050/05, Brussels, 7 November 2005.

- Council of the EU, - *"Withdrawal of Interpol arrest warrant for Mr Zakayev"*, 5810/04, Brussels, 30 January 2004.

- Council of the EU, - *Council Decision fixing the date of application of Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System (SIS II)* - *Council Decision fixing the date of application of Regulation (EC) No 1987/2006 of the establishment, operation and use of the second generation Schengen Information System (SIS II)*, 6937/13, Brussels, 28 February 2013.

- Council of the EU, - *Follow-up to the CAHDATA meeting in Strasbourg 1-3 December 2014*, 5950/15 DCL 1, Brussels, 8 January 2019.

- Council of the EU, - *Notification from Switzerland*, 5409/19, 15 January 2019; the - *Notification from Liechtenstein*, 6696/19, Brussels, 27 February 2019.

- Council of the EU, – *Voting result – Regulation of the European Parliament and of the Council establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/...* – *Adoption of the legislative act 3689th meeting of the Council of the European Union (Agriculture and Fisheries)*, 14 May 2019, 9258/19, Brussels, 14 May 2019.

- Council of the EU, – *"Powers of the EU concerning migration by sea" – "Frontex training" – "Rescue of shipwrecked refugees" – "The dramatic situation of the migrants refused by Malta"*, 11420/07, Brussels, 2 July 2007.

- Council of the EU, – *"Hotspot" approach -FRONTEX support to return of irregular migrants – "Sage countries of origin"*, 10962/15, Brussels, 15 July 2015.

- Council of the EU, *"Interpol warrant against Mr Beslagic"*, 5777/08, Brussels, 29 January 2008.

- Council of the EU, *"EU Agreement on a VISA Information System"*, 11306/03, Brussels, 4 September 2003.

- Council of the EU, *"Media reports of human rights violations by the European border management agency Frontex"*, 16040/09, Brussels, 16 November 2009.

- Council of the EU, *2001 Pro Eurojust Report*, 15545/01, Brussels, 20 December 2001.

- Council of the EU, *2003 IGC – Draft Treaty establishing a Constitution for Europe (following editorial and legal adjustments by the Working Party of IGC Legal Experts) 1*, CIG 50/03, Brussels, 25 November 2003.

- Council of the EU, a) *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member*

States on short-visa b) Council Decision concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member State and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences, 8540/07, Brussels, 18 April 2007.

- Council of the EU, *Access by EUROPOL to the Schengen Information System (SIS), 5970/02, Brussels, 8 February 2002.*

- Council of the EU, *Access for law enforcement purposes to the Entry/Exit System, 11337/1/14 REV 1, Brussels, 16 July 2014.*

- Council of the EU, *Access to the Schengen Information System (SIS) for vehicle registration authorities, 9731/99, Brussels, 12 July 1999.*

- Council of the EU, *Accession of the European Agency for operational management of large-scale IT systems in the area of freedom, security and justice to the Interinstitutional Agreement of 25 May 1999 concerning internal investigations by the European Anti-Fraud Office (OLAF), 14805/12, Brussels, 8 October 2012.*

- Council of the EU, *Activity report of the Europol Joint Supervisory Body (October 1998–October 2002), 13899/03, Brussels, 28 October 2003.*

- Council of the EU, *Activity Report of the Joint Supervisory Body of Eurojust for the year 2008, 12214/09, Brussels, 22 July 2009.*

- Council of the EU, *Activity Report of the Joint Supervisory Body of Eurojust for the year 2005, 11875/06, Brussels, 24 July 2006.*

- Council of the EU, *Adoption of Council Decision authorising the Member States to unanimously approve, on behalf of the European Communities, the adoption by the Committee of Ministers of the Council of Europe of amendments to allow the European Communities to accede to the Convention for the protection of individuals with regard to automatic processing of personal data (Council of Europe Convention 108), 8133/99, Brussels, 20 May 1999.*

- Council of the EU, *Amended Proposal for a Regulation (eu) no .../... of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, 8151/10, Brussels, 30 March 2010.*

- Council of the EU, *Amended proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Asylum and repealing Regulation (EU) No. 439/2010 - A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018, 12112/18, Brussels, 13 September 2018.*

- Council of the EU, *Amended proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) and amending [Regulation (EU) 2018/XX [the Eurodac Regulation],] Regulation (EU) 2018/XX [the Regulation on SIS in the field of law enforcement], Regulation (EU) 2018/XX [the ECRIS-TCN Regulation] and Regulation (EU) 2018/XX [the eu-LISA Regulation]* - Outcome of the European Parliament's first reading (Strasbourg, 15 to 18 April 2019), 7751/19, Brussels, 25 April 2019.

- Council of the EU, *Amended proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) and amending [Regulation (EU) 2018/XX [the Eurodac Regulation],] Regulation (EU) 2018/XX [the Regulation on SIS in the field of law enforcement], Regulation (EU) 2018/XX [the ECRIS-TCN Regulation] and Regulation (EU) 2018/XX [the eu-LISA Regulation]*, 10190/18, Brussels, 15 June 2018.

- Council of the EU, *Amended proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399, Regulation (EU) 2017/2226, Regulation (EU) 2018/XX [the ETIAS Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of border checks] and Regulation (EU) 2018/XX [the eu-LISA Regulation]*, 10178/18, Brussels, 15 June 2018.

- Council of the EU, *Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No. [.../...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No. 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version)*, 14033/12, Brussels, 30 September 2012.

- Council of the EU, *Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] (establishing the criteria and*

mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version) - Opinion of the European Data Protection Supervisor on the amended proposal, 13420/12, Brussels, 6 September 2012.

- Council of the EU, Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version), 11861/12, Brussels, 6 June 2012.

- Council of the EU, Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version) - Analysis of the final compromise text with a view to an agreement, 7713/13, Brussels, 25 March 2003.

- Council of the EU, Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or

a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version), 10638/12, Brussels, 4 June 2012.

- Council of the EU, ANNEX Legislative financial statement to the Proposal for a Regulation of the European Parliament and the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624, 14082/16 ADD 1, Brussels, 16 November 2016.

- Council of the EU, ANNEX to the Recommendation for a Council Decision authorising the opening of negotiations for a cooperation agreement between the European Union and the International Criminal Police Organisation (ICPO-INTERPOL), 7377/21 ADD 1, Brussels, 14 April 2021.

- Council of the EU, Annual report on the 2013 activities of the Central Unit of Eurodac pursuant to Article 24(1) of Regulation (EC) No 2725/2000, 10898/14, Brussels, 12 June 2014.

- Council of the EU, Answers to the additional questionnaire addressed to the new Member States related to - Schengen Information System - Prior consultation, 5602/06 ADD 1 DCL 1, Brussels, 24 May 2018.

- Council of the EU, Approval by the Council of the EU of the draft Memorandum of Understanding between Eurojust and INTERPOL, 11602/13, Brussels, 27 June 2013.

- Council of the EU, Approval by the Council of the EU of the draft Memorandum of Understanding on cooperation between Eurojust and the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), 7628/14, Brussels, 14 March 2014.

- Council of the EU, Article 16b of the Eurojust Decision, 12582/13, Brussels, 19 July 2013.

- Council of the EU, Bringing Member States' national law into conformity with the Decision setting up Eurojust – Discussion paper, 9404/02, Brussels, 14 June 2002.

- Council of the EU, Brussels European Council \ 12 and 13 December 2003 presidency conclusions, 5381/04, Brussels, 5 February 2004.

- Council of the EU, Comments on Articles 27-37 of the Draft Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust), 6981/14, Brussels, 7 March 2014.

- Council of the EU, *Comments on Articles 9-26 of the Draft Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust)*, 18169/13, Brussels, 21 January 2014.

- Council of the EU, *Comments on the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 14609/09, Brussels, 16 October 2009.

- Council of the EU, *Comments on the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 12870/09, Brussels, 2 September 2009.

- Council of the EU, *Commission staff working document accompanying document to the - Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice and - Proposal for a Council decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty - Impact assessment*, 11709/09 ADD 2, Brussels, 3 July 2009.

- Council of the EU, *Commission Staff Working Document Accompanying document to the Proposal for a Regulation of the European Parliament and of the Council establishing an European Asylum Support Office - Impact assessment*, 6700/09 ADD 1, Brussels, 23 February 2009.

- Council of the EU, *Commission Staff Working Document accompanying the Proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] - Impact assessment*, 16934/08, Brussels, 9 December 2008.

- Council of the EU, *Commission staff working document executive summary of the commission staff working document eu-LISA evaluation Accompanying the document Report from the Commission to the European Parliament and the Council on the functioning of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA)*, 10873/17 ADD 2, Brussels, 3 July 2017.

- Council of the EU, *Commission Staff Working Document executive summary of the evaluation Accompanying the document Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the Visa Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation*, 13530/16 ADD 1, Brussels, 21 October 2016.

- Council of the EU, *Commission Staff working document Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)*, 6898/10 ADD 1, Brussels, 1 March 2010.

- Council of the EU, *Commission Staff Working Document Impact Assessment Proposal for a Regulation of the European Parliament and of the Council establishing an entry/exit system to register entry and exit data of third-country nationals crossing the external borders of the Member States of the European Union*, 6928/13 ADD 1, Brussels, 28 February 2013.

- Council of the EU, *Commission staff working document on Implementation of the Eurodac Regulation as regards the obligation to take fingerprints*, SWD(2015) 150 final, 9346/15, Brussels, 29 May 2015.

- Council of the EU, *Commission Staff Working Document on the internal Evaluation of the European Asylum Support Office (EASO)*, 8471/14, Brussels, 2 April 2014.

- Council of the EU, *Commission Staff Working Document, Accompanying the document Report from the Commission to the European Parliament and the Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with articles 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and articles 59 (3) and 66 (5) of Decision 2007/533/JHA*, 15810/16 ADD 1, Brussels, 23 December 2006.

- Council of the EU, *Commission Staff Working Document, Executive Summary of the Impact Assessment, Proposal for a Regulation of the European Parliament and of the Council establishing an entry/exit system to register entry and exit data of third-country nationals crossing the external borders of the Member States of the European Union*, 6928/13 ADD 2, Brussels, 28 February 2013.

- Council of the EU, *Commission Staff Working Documents accompanying document to the Communication from the Commission to the European Parliament the Council, the European Economic and Social Committee of the Regions Report on the evaluation and*

future development of the FRONTEX Agency Impact Assessment, 6664/08 ADD 1, Brussels, 19 February 2008.

- Council of the EU, *Communication from the Commission Legislative package establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 11709/09, Brussels, 3 July 2009.

- Council of the EU, *Communication from the Commission to the Council and the European Parliament on development of the Schengen Information System II*, 5472/02, Brussels, 29 January 2002.

- Council of the EU, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Report on the evaluation and future development of the FRONTEX Agency*, 6664/08, Brussels, 19 February 2008.

- Council of the EU, *Compilation of Member States written contributions*, 6153/1/18 REV 1, Brussels, 16 February 2018.

- Council of the EU, *Conclusions of the Council of the European Union on the way forward to improve information exchange and ensure the interoperability of EU information systems*, 10151/17, Brussels, 14 June 2017.

- Council of the EU, *Conclusions*, 8151/13, Brussels, 5 April 2013.

- Council of the EU, *Council Conclusions on a Common Framework for genuine and practical solidarity towards Member States facing particular pressure on their asylum systems, including though mixed migration flows*, 3151 Justice and Home Affairs Council meeting Brussels, 8 March 2012, and the EU Action on Migratory Pressures - A Strategic Response, 9650/12, Brussels, 10 May 2012.

- Council of the EU, *Council Conclusions on EU Priorities in UN Human Rights Fora in 2021*, 6326/21, Brussels, 22 February 2021.

- Council of the EU, *Council Conclusions on taking the UN-EU strategic partnership on peace operations and crisis management to the next level: Priorities 2022-2024*, 5451/22, Brussels, 24 January 2022.

- Council of the EU, *Council Decision (EU) 2017/1908 of 12 October 2017 on the putting into effect of certain provisions of the Schengen acquis relating to the Visa Information System in the Republic of Bulgaria and Romania (OJ L 269, 19.10.2017, p. 39–43), and the Council Decision on the putting into effect of certain provisions of the Schengen acquis relating to the Visa Information System in the Republic of Bulgaria and Romania - Adoption*, 12411/17, Brussels, 5 October 2017.

- Council of the EU, *Council Decision authorising the opening of negotiations on an arrangement between the European Union, on the one part, and the Republic of Iceland, the Kingdom of Norway, the Swiss Confederation and the Principality of Liechtenstein, on the other part, on the modalities of the participation by those States in the European Agency for the operational management of large-scale information systems in the area of freedom, security and justice, Common Guidelines Consultation deadline*, 17 July 2012, 11797/12, Brussels, 16 July 2012.

- Council of the EU, *Council Decision authorising the opening of negotiations on an arrangement between the European Union, on the one part, and the Republic of Iceland, the Kingdom of Norway, the Swiss Confederation and the Principality of Liechtenstein, on the other part, on the modalities of the participation by those States in the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 11796/12, Brussels, 10 July 2012.

- Council of the EU, *Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences – Bridging Clause*, 8803/07, Brussels, 14 April 2007.

- Council of the EU, *Council Decision concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis relating to the establishment of a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 15766/10, Brussels, 23 November 2010.

- Council of the EU, *Council Decision fixing the date of effect of Decision 2008/633/JHA concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences*, 11431/13, Brussels, 17 July 2013.

- Council of the EU, *Council Decision on setting up a EUROJUST team*, 8938/00, Brussels, 19 June 2000.

- Council of the EU, *Council Decision on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Czech Republic, the Republic of Estonia, the Republic of Latvia, the Republic of Lithuania, the Republic of*

Hungry, the Republic of Malta, the Republic of Poland, the Republic of Slovenia and the Slovak Republic, 8611/07, Brussels, 20 April 2017.

- Council of the EU, *Council Regulation amending Decision 2008/839/JHA on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II)*, 10126/10, Brussels, 2 June 2010.

- Council of the EU, *Council's declaration in Council Decision on the establishment, operation and use of the second generation Schengen Information System (SIS II)*, 10403/07, Brussels, 8 June 2007.

- Council of the EU, *Cover Note, Addition of Denmark to the list of third States with which Europol shall conclude an agreement*, 15759/16, Brussels, 21 December 2016.

- Council of the EU, *Database of missing persons and unidentified bodies – draft EU statement for the Interpol General Assembly*, 11707/1/05 REV 1, Brussels, 8 September 2005.

- Council of the EU, *Development of the Schengen Information System II and possible synergies with a future Visa Information System (VIS)*, 16106/03, Brussels, 15 December 2003.

- Council of the EU, *Development of the Schengen Information System II and possible synergies with a future Visa Information System (VIS)*, 6253/04, Brussels, 13 February 2004.

- Council of the EU, *Development of the Schengen Information System II and possible synergies with a future Visa Information System (VIS)*, 16106/03, Brussels, 15 December 2003.

- Council of the EU, *Development of the Visa System (VIS)*, 14141/04, Brussels, 3 November 2004.

- Council of the EU, *Digitalisation in humanitarian aid: opportunities, challenges and recommendations*, 15048/21, Brussels, 17 December 2021.

- Council of the EU, *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA* 14208/16, 14208/16, Brussels, 9 November 2016.

- Council of the EU, *Discussion Paper from Germany/Europol Drugs Unit – Suggestions for the Improvement of the EU Situation Report on Organised Crime*, 8469/99, Brussels, 19 May 1999.

- Council of the EU, *Discussion paper on the protection of personal data in the Third Pillar of the EU*, 5643/99, Brussels, 4 February 1999.

- Council of the EU, *Document de travail des services de la Commission accompagnant la proposition de règlement du Parlement européen et du Conseil portant création d'un Bureau européen d'appui en matière d'asile - Résumé de l'analyse d'impact*, 6700/09 ADD 2, Brussels, 23 February 2009.

- Council of the EU, *Draft agreement between Eurojust and Europol*, Brussels, 15829/03, 9 December 2003.

- Council of the EU, *Draft Conclusions on the development of the Visa Information System (VIS)*, 6010/04, Brussels, 9 February 2004.

- Council of the EU, *Draft Conclusions on the development of the Visa Information System (VIS)*, 9916/03, 2 June 2003.

- Council of the EU, *Draft conclusions on the improvement of cooperation between Member States, the Commission and FRONTEX with regard to expulsion*, 8329/07, Brussels, 13 April 2007.

- Council of the EU, *Draft Convention concerning the establishment of "Eurodac" for [the taking, recording], comparison [and exchange] of fingerprints of applicants for asylum*, 101/97, Brussels, 15 September 1997.

- Council of the EU, *Draft Council Act drawing up a Protocol extending the scope rationae personae of the Convention on the establishment of "Eurodac" for the comparison of fingerprints of applicants for asylum*, 6324/99, Brussels, 4 March 1998.

- Council of the EU, *Draft Council Conclusions - Strengthening the cooperation and the use of the Schengen Information System (SIS) to deal with persons involved in terrorism or terrorism-related activities, including foreign terrorist fighters - Adoption*, 8974/18, Brussels, 18 March 2018.

- Council of the EU, *Draft Council Conclusions on access to Eurodac by Member States police and law enforcement authorities*, 8688/1/07, Brussels, 16 May 2007.

- Council of the EU, *Draft Council Conclusions on access to Eurodac by Member States police and law enforcement authorities as well as Europol*, 10002, Brussels, 25 May 2007.

- Council of the EU, *Draft Council Conclusions on the Court of Auditors' Special Report No 3/2014 "Lessons from the European Commission's development of the second generation Schengen Information System (SIS II)"*, 12285/14, Brussels, 17 September 2014.

- Council of the EU, *Draft Council Conclusions on the development of the VISA Information System (VIS) Comment to the document 14776/1/03 VISA 187 COMIX 691 REV 1*, 5335/04, Brussels, 15 January 2004.

- Council of the EU, *Draft Council Conclusions on the development of the Visa Information System (VIS)*, 5558/04, Brussels, 26 January 2004.

- Council of the EU, *Draft Council Decision amending the Decision of the Executive Committee set up by the 1990 Schengen Convention, amending the Financial Regulation on the costs of installing and operating the technical support function for the Schengen Information System (C.SIS)*, 13381/09, Brussels, 30 September 2009.

- Council of the EU, *Draft Council Decision authorising the European Commission to participate on behalf of the European Union in the negotiations on the modernisation of Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (EST 108) and the conditions and modalities of accession of the European Union to the modernised Convention*, 7234/3/13 REV 3 EXT 1, Brussels, 25 November 2013.

- Council of the EU, *Draft Council Decision authorising the opening of negotiations for Agreements between the European Union and Algeria, Argentina, Armenia, Bosnia and Herzegovina, Brazil, Colombia, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey on cooperation between the European Union Agency for Criminal Justice Cooperation (Eurojust) and the competent authorities for judicial cooperation in criminal matters of those third States - Adoption*, 5934/21, Brussels, 12 February 2021.

- Council of the EU, *Draft Council Decision authorising the opening of negotiations for a cooperation agreement between the European Union and the International Criminal Police Organization (ICPO-INTERPOL)*, 10261/21, Brussels, 29 June 2021.

- Council of the EU, *Draft Council Decision on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Republic of Croatia*, 8056/17, Brussels, 7 April 2017.

- Council of the EU, *Draft Council Decision setting up Eurojust with a view to reinforcing the fight against serious organised crime*, 13627/00, Brussels, 24 November 2000.

- Council of the EU, *Draft Council Decision setting up Eurojust*, 14052/00, Brussels, 4 December 2000.

- Council of the EU, *Draft Council Decision setting up EUROJUST*, 7408/2/01 REV 2, Brussels, 11 June 2001.

- Council of the EU, *Draft Council Regulation and draft Council Decision on the development of the second generation Schengen Information System (SIS II)*, 13531/01, Brussels, 6 November 2001.

- Council of the EU, *Draft Council Regulation and draft Council Decision on the development of the second generation Schengen Information System (SIS II)*, 11998/01, Brussels, 19 September 2001.

- Council of the EU, *Draft Council Regulation concerning the introduction of some new functions for the Schengen Information System, including the fight against terrorism*, 6874/04, Brussels, 27 February 2007.

- Council of the EU, *Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism*, 8958/04, Brussels, 28 April 2004.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (first reading) - Adoption of the legislative act – Statements*, 12221/18 ADD 1 REV 1, Brussels, 5 October 2018.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System (first reading) - Adoption of the legislative act = statements*, 14091/1/17 REV 1 ADD 1, 15 November 2017.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (first reading) - Adoption of the legislative act = statements*, 14092/1/17 REV 1 ADD 1 14092/1/17 REV 1 ADD 1, Brussels, 15 November 2017.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between the Member States on short-stay visas*, 9423/07 ADD 1, 29 May 2007.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/... (first reading) - Adoption of the legislative act – Statement*, 8733/1/19 REV 1 ADD 1, Brussels, 8 May 2019.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (first reading) - Adoption of the legislative act = statements*, 14092/17 ADD 1, Brussels, 10 November 2017.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System (first reading) - Adoption of the legislative act = statements*, 14091/17 ADD 1, Brussels, 10 November 2017.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union - Access for law enforcement purposes*, 8743/15, Brussels, 19 May 2015.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union*, 10720/14, Brussels, 12 June 2014.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union - Access for law enforcement purposes: Summary and comments by the Presidency regarding answers provided by the Member States to the questionnaire of the former Greek Presidency and discussion on the ways forward*, 13225/14, Brussels, 17 September 2014.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of Visa Information system (VIS) under the Schengen Border Code – Draft statement from the Council meeting*, 13643/08, Brussels, 1 October 2008.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of Visa Information system (VIS) under the Schengen Border Code*, 10109/08, Brussels, 29 May 2008.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of Visa Information system (VIS) under the Schengen Border Code*, 9401/08, Brussels, 16 May 2008.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas – Article 16*, 6531/07, Brussels, 19 February 2007.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas*, 8198/07, Brussels, 2 April 2007.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas*, 6438/07, Brussels, 15 February 2007.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas Chapter III (Articles 16 to 19) and Chapter VII (Articles 36 to 41) – Second reading*, 13663/05, Brussels, 7 November 2005.

- Council of the EU, *Draft Regulation of the European Parliament and the Council concerning the Visa Information System (VIS) and the exchanging of data between the Member States on short-stay visa*, 16229/06, Brussels, 6 December 2006.

- Council of the EU, *Draft Regulation of the European Parliament and the Council concerning the VISA Information System (VIS) and the exchange of data between the Member States on short-stay visas*, 10734/20, Brussels, 4 June 2006.

- Council of the EU, *Draft Regulation of the European Parliament and the Council concerning the Visa Information System (VIS) and the exchange of data between the Member States on short-stay visas*, 9130/06, Brussels, 8 May 2006.

- Council of the EU, *Draft Regulation of the European Parliament and the Council Concerning the Visa Information System (VIS) and the exchange of data between Member States on short-visa*, 11090/05, Brussels, 27 July 2005.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States and short-stay visa*, 8325/06, Brussels, 12 April 2006.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas*, 16225/06, Brussels, 5 December 2006.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-visas*, 8983/05, Brussels, 8 June 2005.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-visas Chapter III (Articles 16 to 19) and Chapter VII (Articles 36 to 41) – Second reading*, 12663/05, Brussels, 7 November 2005.

- Council of the EU, *Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between the Member States on short-stay visa*, 12190/06, Brussels, 7 September 2006.

- Council of the EU, *Draft Regulation of the European Parliament and the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-visa*, 6921/05, Brussels, 16 March 2005.

- Council of the EU, *Draft Statement of the Council's Reasons, Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA – Draft Statement of the Council's reasons*, 14957/15 ADD 1, Brussels, 24 February 2016.

- Council of the EU, *E-POC III and secure communications projects at Eurojust*, 5160/08, Brussels, 15 January 2008.

- Council of the EU, *EASO Annual Report 2012*, 13455/13, Brussels, 17 September 2013.

- Council of the EU, *EASO Work Programme 2013*, 14372/12, Brussels, 2 October 2012.

- Council of the EU, *EASO Work Programme 2014*, 14377/13, Brussels, 7 October 2013.

- Council of the EU, *ECRIS/TCN: Proposal for a Directive amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS) and replacing Council Decision 2009/316/JHA - next steps - debate on crime categories for which fingerprints can be exchanged*, 6691/17, Brussels, 24 February 2017.
- Council of the EU, *Efforts to harmonise the protection of personal data in the third pillar of the EU*, 9084/1/99, Brussels, 11 June 1999.
- Council of the EU, *Eurodac Convention*, Brussels, 28/29.V.1998.
- Council of the EU, *Eurodac Coordinated Supervision Group report on advance deletion*, 18885/11, Brussels, 20 December 2011.
- Council of the EU, *Eurodac implementing rules*, 8140/99, Brussels, 11 May 1999.
- Council of the EU, *EUROJUST/ERA CONFERENCE 10 years of Eurojust Operational Achievements and Future Challenges The Hague, 12-13 November 2012 Outcome Report*, 8862/13, Brussels, 26 April 2013.
- Council of the EU, *Eurojust and the Lisbon Treaty: Towards more effective action Conclusions of the strategic seminar organised by Eurojust and the Belgian Presidency (Bruges, 20-22 September) - Information by the Presidency*, 17625/10, Brussels, 8 December 2010.
- Council of the EU, *EUROJUST Annual Report 2006*, 7550/07, Brussels, 21 March 2007.
- Council of the EU, *EUROJUST Annual Report 2007*, 6866/08, Brussels, 29 February 2008.
- Council of the EU, *EUROJUST Annual Report 2009*, 8147/10, Brussels, 30 March 2010.
- Council of the EU, *EUROJUST Annual Report 2011*, 8853/12, Brussels, 19 April 2012.
- Council of the EU, *EUROJUST Annual Report 2012*, 8179/13, Brussels, 8 April 2013.
- Council of the EU, *EUROJUST Annual Report 2013*, 8151/14, Brussels, 25 March 2014.
- Council of the EU, *EUROJUST Annual Report 2015*, 7492/16, Brussels, 4 April 2016.
- Council of the EU, *EUROJUST Annual Report 2016*, 7971/17, Brussels, 5 April 2017.
- Council of the EU, *EUROJUST Issue in focus number 3 - Cooperation with third States*, 5993/15 ADD 3, Brussels, 19 February 2015.
- Council of the EU, *EUROJUST report to Council on the scope for further measures to improve its capacity to contribute to fight against Terrorism*, 10008/04, Brussels, 1 June 2004
- Council of the EU, *Eurojust-EJN relations*, 1502/02, Brussels, 16 December 2002.

- Council of the EU, *Eurojust-Europol Note, Annual Report to the Council on co-operation between Eurojust and Europol for 2005 and 2006 (Point 2.3 of The Hague Programme)*, 17069/06, Brussels, 21 December 2006.

- Council of the EU, *European Arrest Warrants - Transmission via Interpol*, 6898/05, Brussels, 7 March 2005.

- Council of the EU, *European Parliament plenary session on 15 June 2010 in Strasbourg on the draft Council decision on the application of the provisions of the Schengen acquis relating to the Schengen Information system in the Republic of Bulgaria and Romania*, 11263/10, Brussels, 16 June 2010.

- Council of the EU, *European Union instruments in the field of criminal law and related texts*, Brussels, 2019.

- Council of the EU, *Europol General report 2009*, 10099/10, Brussels, 31 May 2010.

- Council of the EU, *Europol Information System*, 9669/04, Brussels, 24 May 2004.

- Council of the EU, *Europol work programme 2002*, 8141/01, Brussels, 24 April 2001.

- Council of the EU, *Europol's role in the framework of the EU-US TFTP Agreement I and state of play of operational and strategic agreements of Europol (specific focus: the agreement on exchange of personal data and related information that Europol has with the US) - EU information policy on the TFTP Agreement*, 626/11, Brussels, 8 February 2011.

- Council of the EU, *EUROPOL/EU PNR architecture*, 13236/15, Brussels, 22 October 2015.

- Council of the EU, *Evaluation of European Union agencies Endorsement to the Joint Statement and Common Approach*, 1450/12, Brussels, 18 June 2012.

- Council of the EU, *Exchange of views on the final report on mutual evaluation "Exchange of information and intelligence between Europol and the Member States among the Member States respectively"*, 25348/07, Brussels, 20 November 2007.

- Council of the EU, *Exemptions from the fingerprinting requirements in the Visa Information System (VIS)*, 12699/05, Brussels, 28 September 2005.

- Council of the EU, *Exploratory thoughts concerning EUROJUST*, 5700/00, Brussels, 4 February 2000.

- Council of the EU, *Feasibility study SIS one 4all -Schengen Information System*, 13540/06, Brussels, 12 October 2006.

- Council of the EU, *First annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit*, 9319/04, Brussels, 13 May 2004.

- Council of the EU, *Formal comments of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol*, 7114/21, Brussels, 18 March 2021.

- Council of the EU, *Fourth annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit*, 12928/07, Brussels, 14 September 2007.

- Council of the EU, *Frontex Annual Activity Report 2016*, 11442/17, Brussels, 20 July 2017.

- Council of the EU, *Frontex Annual Activity Report 2017*, 10525/18, Brussels, 27 June 2018.

- Council of the EU, *FRONTEX Annual Report 2006*, 11691/07, Brussels, 12 July 2007.

- Council of the EU, *Frontex Annual Report on the implementation on the EU Regulation 656/2014 of the European Parliament and of the Council of 15 May 2014 establishing rules for the surveillance of the external borders*, 11162/15, Brussels, 24 June 2015.

- Council of the EU, *FRONTEX Annual Report*, 12305/09, Brussels, 24 July 2009.

- Council of the EU, *Frontex Annual Risk Assessment 2012*, 10002/12, Brussels, 16 May 2012.

- Council of the EU, *Frontex draft Programming Document 2019 - 2021*, 5247/18, Brussels, 30 January 2018.

- Council of the EU, *Frontex Evaluation Report on return operations - 2nd semester of 2019*, 8920/20, Brussels, 18 June 2020.

- Council of the EU, *Frontex feasibility study on Mediterranean Coastal Patrols Network – MEDSEA*, 12049/06, Brussels, 20 November 2006.

- Council of the EU, *Frontex Programme of Work 2008*, 17440/08, Brussels, 18 December 2008.

- Council of the EU, *Frontex Programme of Work 2010*, 6674/10, Brussels, 23 February 2010.

- Council of the EU, *Frontex Programme of Work 2011*, 5691/11, Brussels, 25 January 2011.

- Council of the EU, *Frontex report on the ETIAS state of preparation*, 7336/20, Brussels, 15 April 2020.

- Council of the EU, *FRONTEX work programme 2007*, 6642/07, Brussels, 22 February 2007.

- Council of the EU, *Frontex Work Programmes 2005 and 2006*, 6941/06, Brussels, 11 July 2006.

- Council of the EU, *Frontex' request of access to Expert FADO and to Expert FADO test environment*, 5669/21, Brussels, 28 January 2021.

- Council of the EU, *General Secretariat of the Council to Marco Cappato (ALDE), "Human rights and Europol-China co-operation agreement"*, 12960/06, Brussels, 18 September 2006.

- Council of the EU, *German comments on the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 14212/09, Brussels, 9 October 2009.

- Council of the EU, *German comments on the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 9802/10, Brussels, 17 May 2010.

- Council of the EU, *Greece's National Action Plan on Asylum Reform and Migration Management = information by Greece, the Commission, Frontex and EASO*, 15358/12, Brussels, 23 October 2012.

- Council of the EU, *Guidelines on Eurojust*, 7384/00, Brussels, 28 March 2000.

- Council of the EU, *High-level expert group on information systems and interoperability. Final report*, Ares(2017) 2412067, Brussels, 11.05.2017.

- Council of the EU, *Horizontal overview of the biometric data quality and format standards to ensure compatibility of different IT systems in the context of interoperability*, 5924/20, Brussels, 20 February 2020.

- Council of the EU, *Horizontal overview of the biometric data quality and format standards to ensure compatibility of different IT systems in the context of interoperability*, 5924/20, Brussels, 20 February 2020.

- Council of the EU, *IGC 2000: Incorporation of a reference to Eurojust in the Treaty*, CONFER 4806/1/00 REV 1, Brussels, 19 November 2000.

- Council of the EU, *IGC 2003 – Non-institutional issues; including amendments in the economic and financial field*, ICG 37/03, Brussels, 24 October 2003.

- Council of the EU, *IGC 2007 Draft declarations*, CIG 3/07, Brussels, 23 July 2007.

- Council of the EU, *Implementation of interoperability: state of play and revised timeline*, 14947/21, Brussels, 13 December 2021.

- Council of the EU, *Improving the use of the Schengen Information System and the Schengen Convention to combat terrorism*, 13920/01, Brussels, 13 November 2001.

- Council of the EU, *Information Note from the Council Legal Service, Judgments of the Court of Justice of 16 April 2015 in Cases C-317/13, C-540/13 and C-679/13 - Annulment of Council Decisions 2013/129/EU and 2013/496/EU (psychoactive substances) and Decision 2013/392/EU (date of effect of the VIS)*, 8541/15, Brussels, 4 May 2015.

- Council of the EU, *Information Technology (IT) measures related to border management a) Systematic checks of external borders b) Entry/Exit System (EES) c) Evolution of the Schengen Information System (SIS) d) EU Travel Information and Authorisation System (ETIAS) e) High-Level Expert Group on Information Systems and Interoperability = Progress report*, 12661/16, Brussels, 3 October 2016.

- Council of the EU, *Information Technology (IT) measures related to border management a) Entry/Exit System (EES) b) EU Travel Information and Authorisation System (ETIAS) = Progress report*, 7064/17, 17 March 2017, p. 3 and the *European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*. - *the issue of the Member State responsible for manual processing of applications*, 7554/17, Brussels, 23 March 2017.

- Council of the EU, *Information Technology (IT) measures related to border management a) Systematic checks of external borders b) Entry/Exit System (EES) c) Evolution of the Schengen Information System (SIS) d) EU Travel Information and Authorisation System (ETIAS) e) High-Level Expert Group on Information Systems and Interoperability = Progress report*, 12661/16, Brussels, 3 October 2006.

- Council of the EU, *Initiative by the Kingdom of Spain with a view to adopting a Council Regulation concerning the introduction of some new functions for the Schengen Information System, in particular in the fight against terrorism*, 13036/02, Brussels, 14 October 2002.

- Council of the EU, *Initiative of the Kingdom of Spain with a view to the adoption of a Council Regulation concerning the introduction of some new functions for the Schengen Information System[, in particular in the fight against terrorism] (document 9407/2/02). Initiative of the Kingdom of Spain with a view to the adoption of a Council Decision concerning the introduction of some new functions for the Schengen Information System [, in particular in the fight against terrorism] (document 9408/2/02)*, 13713/02, Brussels, 5 November 2002.

- Council of the EU, *Interoperability and fundamental rights implications*, 8037/18, Brussels, 18 April 2018.

- Council of the EU, *Interpol discussion paper on the use of Interpol's border security data systems*, 9004/14, Brussels, 15 April 2014.

- Council of the EU, *Involvement of Europol in combatting environmental crime*, 5578/99, Brussels, 1 February 1999.

- Council of the EU, *Joint Declaration of the Commission, the Council and the European Parliament*, 17003/06 ADD 1, Brussels, 19 December 2006.

- Council of the EU, *Joint Europol – Frontex concept note for a possible way forward with regard to the establishment of the horizontal expert group on document fraud*, 10910/17, Brussels, 7 July 2017. *The Situational Overview 2017 prepared by Europol and Frontex as input for the Document Fraud*, 15051/17, Brussels, 4 December 2017.

- Council of the EU, *Joint Supervisory Board's opinion in Council Decision of xx.xx.2001 authorising the Director of Europol to conclude a co-operation agreement between Europol and Interpol*, 8803/01 ADD 2, Brussels, 15 May 2001.

- Council of the EU, *Legislative package establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Location of the seat of the Agency*, 13305/09, Brussels, 15 September 2009.

- Council of the EU, *List of authorities allowed direct access to data stored in the Schengen Information System*, 10495/99, Brussels, 29 July 1999.

- Council of the EU, *List of competent authorities which are authorised to search directly the data contained in the Schengen Information System pursuant to Article 101(4) of the Schengen Convention*, 6265/03, Brussels, 14 April 2003.

- Council of the EU, *Meeting between the Troika of the Article 36 Committee and Interpol Brussels, 16 May 2008*, 10050/08, Brussels, 29 May 2007.

- Council of the EU, *Meeting Document of the Council (Justice, Home Affairs and Civil Protection)*, SN 4038/01, Brussels, 27 and 28 September 2001.

- Council of the EU, *Meeting with Interpol at the level of CATS Brussels, 17 December 2009*, 6386/11, Brussels, 11 February 2010.

- Council of the EU, *Memorandum of Understanding between the European Commission and Eurojust*, 15962/11, Brussels, 24 October 2011.

- Council of the EU, *Mr Wilhelm Schönfelder 12 May 2000 Secretary-General of the Council of the European Union, Mr Javier Solana Communication from the Federal*

Republic of Germany – Initiative by the Federal Republic of Germany regarding a Decision on setting up a EUROJUST team, 8777/00 ADD 1, Brussels, 22 June 2000.

- Council of the EU, Negotiations on the modernisation of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of personal data (EST 108) - Preparation of the CAHDATA meeting on 1-3 December 2014 (Strasbourg), 14780/14 DCL 1, Brussels, 31 October 2019.

- Council of the EU, Negotiations on the modernisation of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of personal data (EST 108) - Preparation of the CAHDATA meeting on 1-3 December 2014 (Strasbourg), 13963/14 DCL 1, Brussels, 30 October 2019.

- Council of the EU, Negotiations on the modernisation of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of personal data (EST 108) - Information with a view to the CAHDATA - meeting on 12-14 November 2013 (Strasbourg), 15850/13 DCL 1, Brussels, 16 November 2018.

- Council of the EU, New JHA working structures: Abolition of CIREFI and transfer of its activities to FRONTEX and the Working Party on Frontiers, 6504/10, Brussels, 22 February 2010.

- Council of the EU, Non-paper by Frontex on its access to central EU systems for borders and security, 15174/17, Brussels, 1 December 2017.

- Council of the EU, Note de Transmission, Document de travail des services de la Commission accompagnant la proposition de règlement du Parlement européen et du Conseil portant création d'un Bureau européen d'appui en matière d'asile – Résumé de l'analyse d'impact, 6700/09 ADD 2, Brussels, 23 February 2009.

- Council of the EU, Note from the French authorities on Article 54 (bilateral agreements) of the draft Regulation establishing an Entry/Exit System, 14562/16, 18 November 2016. Law enforcement access to EES and bilateral agreements were already the last two points of discussions until the end, see the Entry Exit (EES): a) Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of, entry data of third country nationals crossing the external borders of Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011 b) Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 2016/399 as

regards the use of the Entry/Exit System - Progress report, 15350/16, Brussels, 7 December 2016.

- Council of the EU, *Note of the Commission, Explanatory note the Europol mechanism under the draft TFTP mechanism*, 130/10, Brussels, 18 June 2010.

- Council of the EU, *Note of the French Delegation, Status of information copied to Europol pursuant to Article 6(2) of the Framework Decision 2006/960/JHA*, 15408/08, Brussels, 10 November 2008.

- Council of the EU, *Note of the Secretariat General of the Council of the European Union on the Declaration on combating terrorism*, 7906/04, Brussels, 9 March 2004.

- Council of the EU, *Note sent by the Spanish delegation sent to the Visa Working Party on Databases of visas*, 15577/01, Brussels, 21 December 2001.

- Council of the EU, *Note to Initiative, Slovenia, the French Republic, the Czech Republic, the Kingdom of Sweden, the Kingdom of Spain, the Kingdom of Belgium, the Republic of Poland, the Italian Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Slovak Republic, the Republic of Estonia, the Republic of Austria and the Portuguese Republic* 7 January 2007, 5038/08, Brussels, 30 January 2008,

- Council of the EU, *Notification from the United Kingdom concerning its intention to take part in the adoption of the Council Regulation (EC) concerning the establishment of "EURODAC" for the comparison of fingerprints of applicants for asylum and certain other aliens*, 11870/1/99 REV 1, Brussels, 18 October 1999.

- Council of the EU, *Notification from UK to participate in the adoption and application of the Council Decision authorising the opening of negotiations on an arrangement between the European Union, on the one part, and the Republic of Iceland, the Kingdom of Norway, the Swiss Confederation and the Principality of Liechtenstein, on the other part, on the modalities of the participation by those States in the European Agency for the operational management of large-scale information systems in the area of freedom, security and justice*, 12128/12, Brussels, 6 July 2012.

- Council of the EU, *Notifications to Eurojust of breaches of time limits in the execution of European Arrest Warrants (Article 17(7) (first sentence) of FD on EAW)*, 10270/14, Brussels, 26 May 2014.

- Council of the EU, *Opinion 116/2005 on the Proposals for a Regulation of the European Parliament and of the Council (COM (2005) 236 final) and a Council Decision (COM (2005) 230 final) on the establishment, operation and use of the second generation Schengen information system (SIS II) and a Proposal for a Regulation of the European Parliament and*

of the Council regarding access to the second generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM (2005) 237 final), 14967/05, Brussels, 11 January 2006.

- Council of the EU, Opinion 7/2017 on the new legal basis of the Schengen Information System, 9412/17, Brussels, 17 May 2017.

- Council of the EU, Opinion of Eurojust I on the practical implementation of Articles 26(2) last sentence, 26a(2) last sentence and 27a(1) of the revised Eurojust Decision, 12479/10, Brussels, 22 July 2010.

- Council of the EU, Opinion of the EDPS - on the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and - on the proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty, 5039/10, Brussels, 7 January 2010.

- Council of the EU, Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX), 10127/10, Brussels, 25 May 2010.

- Council of the EU, Opinion of the European Data Protection Supervisor on the legislative proposals concerning the Second Generation Schengen Information System (SIS II), 14091/05, Brussels, 14 November 2005.

- Council of the EU, Opinion of the European Data Protection Supervisor on the Proposal for Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011, 13188/17, Brussels, 13 October 2017.

- Council of the EU, Opinion of the European Data Protection Supervisor on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme, 10679/13, Brussels, 24 July 2013.

- Council of the EU, Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by

Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, 7599/06, Brussels, 20 March 2006.

- Council of the EU, *Opinion of the European Data Protection Supervisor on the Amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person]*, and on the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, 14416/09, Brussels, 16 October 2009.

- Council of the EU, *Opinion of the European Data Protection Supervisor on the proposal for a Council Regulation on migration from the Schengen Information System (SIS) to the second generation Schengen Information System (SIS II) (recast)*, 12530/12, Brussels, 12 July 2012.

- Council of the EU, *Opinion of the European Data Protection Supervisor on the legislative proposals concerning the Second Generation Schengen Information System (SIS II)*, 14091/05, Brussels, 14 November 2005.

- Council of the EU, *Opinion of the Joint Supervisory Body of Eurojust regarding data protection in the proposed new Eurojust legal framework*, 17419/13, Brussels, 6 December 2013.

- Council of the EU, *Opinion of the Legal Service, Draft EY Framework Decision on the protection of the environment through criminal law – Compliance with Community powers (Article 47 of the TEU)*, 6793/01, Brussels, 8 March 2001.

- Council of the EU, *Opinion on the Possibility of including data on illegal migrants in the Eurodac system*, 5754/98, Brussels, 16 March 1998.

- Council of the EU, *Opinion on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, 10484/18, Brussels, 27 June 2018.

- Council of the EU, *Options for the establishment of the legal basis for the provisions of the Schengen acquis relating the Schengen Information System*, 11561/98, Brussels, 26 October 1998.

- Council of the EU, *Policy document concerning access to Eurodac by Member States' police and law enforcement authorities*, 16982/06, Brussels, 20 December 2006.

- Council of the EU, *Position en première lecture adoptée par le Conseil le 25 février 2010 en vue de l'adoption du règlement du Parlement européen et du Conseil portant création d'un Bureau européen d'appui en matière d'asile = Exposé des motifs du Conseil*, 16626/2/09 REV 2 ADD 1, Brussels, 25 February 2010.

- Council of the EU, *Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council amending Regulations (EU) No 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 and (EU) 2019/818 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the Visa Information System – Draft Statement of the Council's reasons*, 5951/21 ADD 1, Brussels, 20 May 2021.

- Council of the EU, *Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System – Statement of the Council's reasons – Adopted by the Council on 27 May 2021*, 5950/1/21 REV 1 ADD 1, Brussels, 28 May 2021.

- Council of the EU, *Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System – Draft Statement of the Council's reasons*, 5950/21 ADD 1, Brussels, 20 May 2021.

- Council of the EU, *Possible cooperation between Eurojust and the Council Working Party on Legal Data Processing (e-Justice) regarding the development of common standards for the exchange of data in the judicial domain*, 8991/10, Brussels, 30 April 2010.

- Council of the EU, *Preliminary draft reply to question for written answer e-009274/2014 - Marina Albiol Guzmán (GUE/NGL) Role of the Council in negotiating Interpol Resolution AG-2010-RES-10*, 6000/15, Brussels, 9 February 2015.

- Council of the EU, *Preparation of the Schengen evaluation of the new Member States – Letter to the Frontex Agency: Request for risk analysis*, 12222/05, Brussels, 18 October 2005.

- Council of the EU, *Presidency Note, Europol and External Relations*, 7153/04, Brussels, 8 March 2004.

- Council of the EU, *Presidency Note, Exchange of letters related to the Supplemental Agreement between the United States of America and Europol on the exchange of personal data and related information -Opinion of the Europol Joint Supervisory Body*, 1396/1/02 REV1, Brussels, 28 November 2002.

- Council of the EU, *Presidency project for a system of electronic recording of entry and exit dates of third-country nationals in the Schengen area*, 13403/08, Brussels, 24 September 2008.

- Council of the EU, *Presidency project for a system of electronic recording of entry and exit dates of third-country nationals in the Schengen area*, 13403/08 ADD 1, Brussels, 25 September 2008.

- Council of the EU, *Presidency project for a system of electronic recording of entry and exit dates of third-country nationals in the Schengen area*, 13403/08 ADD 2, Brussels, 25 September 2008.

- Council of the EU, *Presidency project for a system of electronic recording of entry and exit dates of third-country nationals in the Schengen area*, 13403/08 ADD 3, Brussels, 15 October 2008.

- Council of the EU, *Presidency project for a system of electronic recording of entry and exit dates of third-country nationals in the Schengen area*, 14334/08, Brussels, 16 October 2008.

- Council of the EU, *Presidency project for a system of electronic recording of entry and exit dates of third-country nationals in the Schengen area*, 13403/08 ADD 4, Brussels, 20 October 2008.

- Council of the EU, *Presidency project for a system of electronic recording of entry and exit dates of third-country nationals in the Schengen area*, 13403/08 ADD 5, Brussels, 21 October 2008.

- Council of the EU, *Presidency project for a system of electronic recording of entry and exit dates of third-country nationals in the Schengen area*, 12251/08, Brussels, 28 June 2008.

- Council of the EU, *Presidency Report on the activity of the Europol Drugs Unit/Europol 1998*, 6190/99, Brussels, 19 February 1999.

- Council of the EU, *Presidency's Note, Conclusions from the Expert Meeting on the Follow-up of the Joint Frontex Europol Report on the High Risk Routes of Illegal Migration*

in the Western Balkan Countries within the Frontex Risk Analysis Network, 5685/08, Brussels, 15 February 2008.

- Council of the EU, *Presidency's Note, Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA - Discussion paper on Europol's agreements with third countries, 13702/13, Brussels, 17 September 2013.*

- Council of the EU, *President of Eurojust to the Chair of the DAPIX Working Party, 6127/18, Brussels, 14 February 2018.*

- Council of the EU, *Proposal for a Council common position on: Draft Regulation of the European Parliament and of the Council amending the provisions of the Convention implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at common borders as regards access to the Schengen Information System by the authorities and services in the Member States responsible for issuing registration certificates for vehicles, 13824/04, Brussels, 22 October 2004.*

- Council of the EU, *Proposal for a COUNCIL DECISION authorising Member States to ratify, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), 9766/18, Brussels, 6 June 2018.*

- Council of the EU, *Proposal for a COUNCIL DECISION authorising Member States to sign, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No.108) - Outcome of the DAPIX meeting on 15 June 2018, 10225/18, Brussels, 18 June 2018.*

- Council of the EU, *Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences – proposals for re-drafting, 14196/1/06, Brussels, 23 November 2006.*

- Council of the EU, *Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, 10290/07, Brussels, 8 June 2007.*

- Council of the EU, *Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of the Member States responsible for internal Security and by Europol for the purposes of the prevention, detection and investigation of the terrorist offences and of other serious criminal offences – Schengen relevance*, 9317/06, 15 May 2006.

- Council of the EU, *Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences*, 14196/2/06, Brussels, 22 December 2006.

- Council of the EU, *Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences*, 14196/06, Brussels, 19 October 2006.

- Council of the EU, *Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences*, 15142/05, Brussels, 20 November 2005.

- Council of the EU, *Proposal for a Council Decision establishing the Visa Information System (VIS)*, 6373/04, Brussels, 16 February 2004.

- Council of the EU, *Proposal for a Council Decision on the establishment, operation and use of the second generation Schengen information system (SIS II)*, 9942/05, Brussels, 9 June 2005.

- Council of the EU, *Proposal for a Council Regulation amending the Convention Implementing the Schengen Agreement as regards long-stay visas and alerts in the Schengen Information System*, 7094/09, Brussels, 2 March 2009.

- Council of the EU, *Proposal for a Council Regulation concerning the establishment of 'Eurodac' for the comparison of fingerprints of applicants for asylum and certain other aliens*, 11396/99, Brussels, 1 October 1999.

- Council of the EU, *Proposal for a Council Regulation concerning the establishment of "Eurodac" for the comparison of fingerprints of applicants for asylum and certain other aliens*, 10530/99, Brussels, 2 August 1999.

- Council of the EU, *Proposal for a Council Regulation concerning the establishment of 'Eurodac' for the comparison of fingerprints of applicants for asylum and certain other aliens*, 11683/99, Brussels, 8 October 1999.

- Council of the EU, *Proposal for a Council Regulation on migration from the Schengen Information System (SIS I+) to the second generation Schengen Information System (SIS II) (recast)*, 14003/12, Brussels, 20 September 2012.

- Council of the EU, *Proposal for a Council Regulation on migration from the Schengen Information System (SIS I+) to the second generation Schengen Information System (SIS II)*, 13463/12, Brussels, 7 September 2012.

- Council of the EU, *Proposal for a Council Regulation on migration from the Schengen Information System (SIS I+) to the second generation Schengen Information System (SIS II) (recast) – New data categories and functionalities in SIS II*, 13057/12, Brussels, 31 July 2012.

- Council of the EU, *Proposal for a Directive of the Council and the European Parliament on the use of Passenger Name Record for the prevention, detection, investigation and prosecution of terrorist offences and serious crime - possible role for Europol*, 12142/15, Brussels, 23 September 2015.

- Council of the EU, *Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data – Chapters V and X*, 6846/14 ADD 1, Brussels, 25 February 2014.

- Council of the EU, *Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, 7979/15, Brussels, 16 April 2015.

- Council of the EU, *Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data - Chapters V-VI*, 6846/14 ADD 3, Brussels, 28 March 2014.

- Council of the EU, *Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by*

competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 16497/12 ADD 2, Brussels, 7 December 2012.

- Council of the EU, *Proposal for a draft Council Decision on the Establishment, Operation and Use of the Second Generation Schengen Information System (SIS II) – Revised proposal*, 5710/4/06 REV 4 ADD 1, Brussels, 17 July 2006.

- Council of the EU, *Proposal for a draft Council Decision on the Establishment, Operation and Use of the Second Generation Schengen Information System (SIS II) – Redrafted proposal*, Brussels, 5710/06, 27 January 2006.

- Council of the EU, *Proposal for a Regulation establishing an Entry/Exit System (EES) – Territorial scope of application of the EES in the light of Article 6(1) of the Schengen Borders Code for the purpose of calculating the short-stay (90 days in any 180-day period)*, 3491/16, Brussels, 19 October 2016.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Asylum and repealing Regulation (EU) No. 439/2010*, 12701/16, Brussels, 5 October 2016.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Asylum and repealing Regulation (EU) No. 439/2010 – State of play and guidance for further work*, 9563/17, Brussels, 29 May 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Asylum and repealing Regulation (EU) No. 439/2010 (First reading) – Letter to the Chair of the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE)*, 10352/21, Brussels, 30 June 2021.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Asylum and repealing Regulation (EU) No. 439/2010*, 10517/16, Brussels, 6 October 2016.

- Council of the EU, *Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)*, 8861/11, Brussels, 13 April 2021.

- Council of the EU, *Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)*, 6898/10, Brussels, 1 March 2010.

- Council of the EU, *Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)*, 17451/10, Brussels, 13 December 2010.

- Council of the EU, *Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 207/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)*, 10538/10, Brussels, 9 June 2010.

- Council of the EU, *Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) – the necessity for FRONTEX to process personal data*, 15337/10, Brussels, 28 October 2010.

- Council of the EU, *Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) - Personal data related issues*, 13466/10, Brussels, 14 September 2010.

- Council of the EU, *Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 207/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)*, 10594/11, Brussels, 26 May 2011.

- Council of the EU, *Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 207/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)- Analysis of the final compromise text with the view to agreement*, 12341/1, Brussels, 5 July 2011.

- Council of the EU, *Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No 207/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)*, 968/10, Brussels, 1 May 2010.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust) -*

Invitation to Eurojust to provide a written contribution to the Working Party on Cooperation in Criminal Matters COPEN (Eurojust Regulation), 8488/14, Brussels, 4 April 2014.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation – mandate for negotiations with the European Parliament*, 10414/21, Brussels, 25 October 2021.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol – Mandate for negotiations with the European Parliament*, 12800/21, Brussels, 13 October 2021.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No. 45/2001 and Decision No. 1247/2002 [First reading] - Compilation of Member States written contributions*, 6153/1/18, Brussels, 16 February 2018.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No. 45/2001 and Decision No. 1247/2002 [First reading] - Presidency suggestions*, 5580/18, Brussels, 31 January 2018.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA - Data protection supervisory bodies for Europol*, 15495/13, Brussels, 31 October 2013.

- Council of the EU, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Applicability of the General Data Protection Regulation to the activities of the International Committee of the Red Cross (ICRC)*, 7355/15, Brussels, 25 March 2015.

- Council of the EU, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Applicability of*

the General Data Protection Regulation to the activities of the International Committee of the Red Cross (ICRC), 8837/15, Brussels, 12 May 2015.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 - Examination of the Presidency revised text, 7651/18, Brussels, 13 April 2018.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of, entry data of third country nationals crossing the external borders of Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011. Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 2016/399 as regards the use of the Entry/Exit System - Mandate for negotiations with the European Parliament, 6572/17 COR 1, Brussels, 2 March 2017.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011 Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 2016/399 as regards the use of the Entry/Exit System - Territorial scope of the application of the EES and the calculation of the duration of the short-stay - guidance for further work, 5565/17, Brussels, 24 January 2017.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of, entry data of third country nationals crossing the external borders of Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011 - Explanation of the functioning of Article 3a of the EES proposal, 15351/16, Brussels, 8 December 2016.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal

of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011, 9387/16, Brussels, 26 May 2006.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011, 8421/16, Brussels, 2 May 2016.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011, 8518/16, Brussels, 4 May 2016.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System - The calculation of the duration of stay in the framework of the automated calculator, 11893/16, Brussels, 9 September 2016.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third-country nationals - Schengen relevance, 10768/17, Brussels, 28 June 2017.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), 15729/17, Brussels, 14 December 2017.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011 - General approach, 14807/17, Brussels, 24 November 2017.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third

country nationals crossing the external borders of the Member States of the European Union, 6928/13, Brussels, 28 February 2003.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Compromise version, 16282/09 ADD 1, Brussels, 20 November 2009.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Compromise version, 16282/09 ADD 7, Brussels, 3 December 2009.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011 – Outcome of the European Parliament's first reading (Strasbourg 2 to 5 July 2018), 10714/18, Brussels, 12 July 2018.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice - seat of the Agency, 5285/10, Brussels, 13 January 2010.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice - seat of the Agency, 14469/10, Brussels, 25 October 2010.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice - seat of the Agency, 17287/10, Brussels, 1 December 2010.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, 10827/2/11, REV 2 ADD 1, Brussels, 8 June 2011.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems

in the area of freedom, security and justice, 10827/2/11, REV 2 ADD 3, Brussels, 8 June 2011.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (first reading) – Adoption of the legislative act* = *Statements*, 13136/2/11 REV 2 ADD 1, Brussels, 9 September 2011.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Revised compromise version*, 5747/10 ADD 1, Brussels, 1 February 2010.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Compromise version*, 16282/09 ADD 3, Brussels, 20 November 2009.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – seat of the Agency*, 5038/10, Brussels, 7 January 2010.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Draft compromise text*, 8269/10, Brussels, 7 April 2010.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice - input based on the Information Management Strategy*, 14838/09, Brussels, 26 October 2009.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 14995/09, Brussels, 27 October 2009.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011 – Revised draft*, 11884/17, Brussels, 13 September 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011 – Third revised draft*, 13128/17, Brussels, 23 October 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Possible agreement with the EP*, 10827/11, Brussels, 30 May 2011.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Compromise version*, 16282/09 ADD 4, Brussels, 20 November 2009.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – Open issues – Preparation of the informal trilogue*, 14469/10, Brussels, 25 October 2010.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011*, 10820/17, Brussels, 30 June 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice - Preparation for the high-level trialogue*, 7638/11, Brussels, 11 March 2011.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European criminal records information system (ECRIS-TCN system) and amending Regulation (EU) No. 1077/2011 - Confirmation of the final compromise text with a view to agreement*, 15701/18, Brussels, 18 December 2018.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding*

conviction information on third country nationals and stateless persons (TCN) to supplement and support the European criminal records information system (ECRIS-TCN system) and amending Regulation (EU) No. 1077/2011 [First reading] - Policy debate, 12596/17, Brussels, 2 October 2017.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011 - Presidency note, 11310/18, Brussels, 6 September 2018.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011 - Presidency note with questions, 10828/18, Brussels, 10 July 2018.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU No 1077/2011) - Four column table with Presidency suggestions/comments, 5505/18, Brussels, 9 February 2018.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU No 1077/2011) - Revised four column table, 7521/18, Brussels, 12 April 2012.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European criminal records information system (ECRIS-TCN system) and amending Regulation (EU) No. 1077/2011 - Revised text following COPEN meeting on 11 and 12 September 2017, 12187/17, Brussels, 19 September 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European criminal records information system (ECRIS-TCN system) and amending Regulation (EU) No. 1077/2011 - Thematic discussion paper*, 12574/17, Brussels, 4 October 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011*, 10940/17, Brussels, 3 July 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European criminal records information system (ECRIS-TCN system) and amending Regulation (EU) No. 1077/2011 - Summary of the proceedings of the COPEN meeting on 18 July 2017*, 11445/17, Brussels, 31 August 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorization System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*, 8584/17, Brussels, 10 May 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*, 6929/17, Brussels, 8 March 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*, 7152/18, Brussels, 22 March 2018.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*, 10017/17 ADD 1, Brussels, 13 June 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing the conditions for accessing other EU information systems for ETIAS purposes and amending Regulation (EU) 2018/1240, Regulation (EC) No 767/2008, Regulation (EU) 2017/2226 and Regulation (EU) 2018/1861* Proposal for a Regulation of the European Parliament and of the Council establishing the conditions for accessing the other EU information systems and amending Regulation (EU) 2018/1862 and Regulation (EU) yyyy/xxx [ECRIS-TCN] Comments of the European Data Protection Supervisor, 7553/19, Brussels, 15 March 2019.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/162*, 9349/17, Brussels, 19 May 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*, 13907/17, Brussels, 17 November 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*, 15127/17, Brussels, 15 December 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS)*, 6324/17, Brussels, 20 February 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*, 8231/17, Brussels, 12 April 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*, 8701/16, Brussels, 12 May 2016.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*, 12476/16, Brussels, 12 September 2016.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*, 10880/16, Brussels, 6 July 2016.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*, 10113/1/17 REV 1, Brussels, 15 June 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*, 8446/16, Brussels, 2 May 2016.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of, entry data of third country nationals crossing the external borders of Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011. Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 2016/399 as regards the use of the Entry/Exit System - Partial mandate to open interinstitutional negotiations with the European Parliament*, 15063/16, Brussels, 6 December 2016.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011* Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 2016/399 as regards the use of the Entry/Exit System - Preparation of further steps, 14700/16, Brussels, 24 November 2016.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*, 9578/16, Brussels, 31 May 2016.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of, entry data of third country nationals crossing the external borders of Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011 - Article 38 and 38a*, 10114/17, Brussels, 8 June 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of, entry data of third country nationals crossing the external borders of Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011 - Article 38 and 38a*, 10361/17, Brussels, 15 June 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP)*, 6931/13, Brussels, 28 February 2013.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union*, 11143/13, Brussels, 20 June 2013.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP), Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme*, 10704/13, Brussels, 10 June 2013.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union*, 15969/13, Brussels, 18 November 2013.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union – Access for law enforcement purposes: Summary of the replies to the questionnaire*, 13680/13, Brussels, 10 October 2013.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union – Questionnaire*, 12107/13, 15 July 2013.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union – Questionnaire*, 14066/13, Brussels, 1 October 2013.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union*, 17536/13, Brussels, 13 December 2013.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA –*

Amendment to the mandate for negotiations with the European Parliament, 8787/20, Brussels, 17 June 2020.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA - Mandate for negotiations with the European Parliament, 15726/18, Brussels, 19 December 2018.*

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Borders Code – Outcome of the European Parliament's first reading (Brussels, 1 to 4 September 2008), 12704/08, Brussels, 15 September 2008.*

- Council of the EU, *Proposal for a Regulation of the European Parliament and the Council concerning the Visa Information System (VIS) and the exchanging of data between the Member States on short-stay visa, 5093/05, Brussels, 4 January 2004.*

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast) – Preparation for the trilogue, 9848/18, Brussels, 12 June 2018.*

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU)*

1077/2011 establishing a European Agency for the operational management of large- scale IT systems in the area of freedom, security and justice (recast), 15166/1/16, REV 1, Brussels, 2 December 2016.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] , for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast), 10531/16, Brussels, 8 July 2016.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], Annex, 16934/08, Brussels, 9 December 2008.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No. 515/2014 and repealing Regulation (EC) No. 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU, 15814/16, Brussels, 23 December 2006.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II), 14498/05, Brussels, 16 November 2005.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II) – Redrafted proposal, 5709/1/06 TEV 1 ADD 6, Brussels, 4 April 2006.

- Council of the EU, Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II), 5709/3/06 REV 3, Brussels, 24 April 2006.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II)* - Legal Base, 11380/05, Brussels, 20 July 2005.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen information system (SIS II)* – Outcome of the European Parliament's first reading (Strasbourg, 23 to 26 October 2006), 14296/06, Brussels, 27 October 2006.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates*, 9944/05, Brussels, 9 June 2005.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen information system (SIS II)*, 9943/05, Brussels, 9 June 2005.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas* - Legal basis, 6683/05, Brussels, 23 February 2005.

- Council of the EU, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, 5853/12, Brussels, 27 January 2012.

- Council of the EU, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* – Partial General Approach on Chapter V, 10349/14, Brussels, 28 May 2014.

- Council of the EU, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* - Partial General Approach on Chapter V, 10349/14 COR 1, Brussels, 11 June 2014.

- Council of the EU, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* – Comments on Chapter V, 6723/13, 26 February 2013.

- Council of the EU, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* - Comments on Chapter V, 6723/5/13 REV5, Brussels, 12 December 2013.

- Council of the EU, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* -Proposals regarding Chapter V, 10198/14, Brussels, 23 May 2014.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third-country nationals* - Schengen relevance, 10768/17, Brussels, 28 June 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union*, 6928/13, Brussels, 28 February 2003.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] , for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast)* - Inclusion of colour copies of passport or ID documents in Eurodac, 8221/17, Brussels, 12 April 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624* - Information of the European Parliament on the splitting of the original proposal into two texts, 10364/17, Brussels, 23 June 2017.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)* - Presidency revised text of provisions specific to this Regulation, 6551/18, Brussels, 28 February 2018.

- Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council establishing the conditions for accessing the other EU information systems and amending Regulation (EU) 2018/1862 and Regulation (EU) yyyy/xxx [ECRIS-TCN]* - *Opt-in by the United Kingdom*, 8809/19, Brussels, 24 April 2019.

- Council of the EU, *Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust) - provisions on data protection (Presidency proposal)*, 10633/17, Brussels, 23 June 2017.

- Council of the EU, *Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust) - discussion paper on the Data Protection Supervision Regime for Eurojust*, 11993/17, Brussels, 11 September 2017.

- Council of the EU, *Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust) - Third Opinion of the Joint Supervisory Body of Eurojust*, 8638/15, Brussels, 8 May 2015.

- Council of the EU, *Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (EUROJUST) - Provisions relating to the European Public Prosecutor's Office*, 5730/15, Brussels, 2 February 2015, and *Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust) - Confidentiality and Security Rules (Articles 59 and 62)*, 5916/15, Brussels, 10 February 2015.

- Council of the EU, *Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust) - Written comments by Czech Republic on Articles 1 - 21 of the Draft Regulation*, 13631/14, Brussels, 29 September 2014.

- Council of the EU, *Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (EUROJUST) and the Proposal for a Regulation on the European Agency for Law Enforcement Cooperation (EUROPOL)*, 11682/14, Brussels, 9 July 2014.

- Council of the EU, *Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (EUROJUST) - Orientation debate*, 9486/14, Brussels, 19 May 2014.

- Council of the EU, *Proposal of a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-visa – Outcome of the European Parliament's first reading (Brussels, 6 to 7 June 2007)*, 9753/07, Brussels, 19 June 2007.

- Council of the EU, *Proposal of the incoming Spanish Presidency and Europol's initiative for the establishment of a monitoring centre on cyber crime at Europol*, 15456/01, Brussels, 18 December 2001.

- Council of the EU, *Proposal to the Council regarding rules of procedure on the processing and protection of Personal data at Eurojust*, 14439/04 ADD 2, Brussels, 28 January 2005.

- Council of the EU, *Proposal to the Council regarding rules of procedure on the processing and protection of Personal data at Eurojust*, 14439/04, Brussels, 12 November 2004.

- Council of the EU, *Proposals from Europol: Improving information and intelligence exchange in the area of counter terrorism across the EU*, 7272/15, Brussels, 16 March 2015.

- Council of the EU, *Proposition de règlement du Parlement européen et du Conseil amendant le règlement (UE) 2016/399 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes - Compromis partiel de la présidence*, Brussels, 6366/22, 18 February 2022.

- Council of the EU, *Proposition de Règlement du Parlement Européen et du Conseil modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation – Préparation du trilogue*, 5370/22, Brussels, 24 January 2022.

- Council of the EU, *Questionnaire on the possible creation of a system of electronic recording of entries and exits of third country nationals in the Schengen area*, 8552/09, Brussels, 21 April 2009.

- Council of the EU, *Recommendation for a COUNCIL DECISION authorising the opening of negotiations for a cooperation agreement between the European Union and the International Criminal Police Organisation (ICPO-INTERPOL)*, 9915/21, Brussels, 18 June 2021.

- Council of the EU, *Recommendation for a Council Decision authorising the opening of negotiations on the modernisation of Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (EST 108) and the conditions and modalities of accession of the European Union to the modernised Convention*, 6176/13 DCL 1, Brussels, 30 January 2019.

- Council of the EU, *Recommendation for a COUNCIL DECISION authorising the opening of negotiations on the modernisation of Council of Europe Convention for the*

protection of individuals with regard to automatic processing of personal data (EST 108) and the conditions and modalities of accession of the European Union to the modernised Convention, 16466/12 EXT 1, Brussels, 6 February 2014.

- Council of the EU, *Recommended guidelines for data security in connection with Schengen Information System, 11148/1/02, Brussels, 18 October 2002.*

- Council of the EU, *Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 - Notification from Denmark, 10999/18, Brussels, 10 July 2018.*

- Council of the EU, *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (recast), 8474/09, Brussels, 14 April 2009.*

- Council of the EU, *Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (recast), 7649/09, Brussels, 2 April 2009.*

- Council of the EU, *Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU - draft compromise text regarding alerts on persons and objects for discreet checks, inquiry checks or specific checks (Articles 36 and 37), 8411/17, Brussels, 26 April 2017.*

- Council of the EU, *Report from the Commission to the European Parliament and the Council on the functioning of the European Agency for the operational management of*

large-scale IT systems in the area of freedom, security and justice (eu-LISA) Council of the European Union, 10873/17, Brussels, 3 July 2017.

- Council of the EU, *Report from the commission to the European Parliament and the Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and art. 59 (3) and 66 (5) of Decision 2007/533/JHA*, 15810/16, Brussels, 23 December 2006.

- Council of the EU, *Report from the Commission to the European Parliament and the Council on the state of play of preparations for the full implementation of the new legal bases for the Schengen Information System (SIS) in accordance with Article 66(4) of Regulation (EU) 2018/1861 and Article 79(4) of Regulation (EU) 2018/1862*, 6463/20, Brussels, 28 February 2020.

- Council of the EU, *Report from the Commission to the European Parliament and the Council, The availability and readiness of technology to identify a person on the basis of fingerprints held in the second generation Schengen Information System (SIS II)*, 6720/16, Brussels, 2 March 2016.

- Council of the EU, *Report from the Eurojust Seminar on the new draft Regulation on Eurojust: "an improvement in the fight against cross-border crime?", The Hague, 14-15 October 2013*, 17188/1/13 REV 1, Brussels, 4 December 2013.

- Council of the EU, *Report of the Europol Joint Supervisory Board in the Council of the EU*, 13899/03, Brussels, 28 October 2003.

- Council of the EU, *Report on cooperation between Frontex, the European Border and Coast Guard Agency and third countries in 2019*, 8896/20, Brussels, 17 June 2020.

- Council of the EU, *Report on the annual accounts of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) for the financial year 2013 together with the Agency's replies*, 16479/14, Brussels, 5 December 2014.

- Council of the EU, *Request from Ireland to take part in the Regulation of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 8510/12, Brussels, 3 April 2012.

- Council of the EU, *Resolution of the European Parliament on the strategic priorities for the Commission's work programme for 2017*, 2016/2773 (RSP), Brussels, 6 July 2016.

- Council of the EU, *Restrictions on the use of Eurodac Data*, 12697/04, Brussels, 23 September 2003.

- Council of the EU, *Roadmap of 6 June 2016 to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area* —, 9368/1/16 REV 1, Brussels, 6 June 2016.

- Council of the EU, *Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area: - State of play of its implementation (third implementation report)*, 7931/1/18 REV 1, Brussels, 22 June 2016.

- Council of the EU, *Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area: - Update following Council Conclusions on interoperability*, 14750/17, Brussels, 24 November 2017.

- Council of the EU, *Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area: - State of play of its implementation (second implementation report)*, 8433/17, Brussels, 11 May 2017.

- Council of the EU, *Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area: - State of play of its implementation*, 13554/1/16 REV 1, Brussels, 8 November 2016.

- Council of the EU, *Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area*, 7711/16, Brussels, 12 April 2016.

- Council of the EU, *Schengen Information System (SIS) – Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) for the return of illegally staying third-country nationals* – *Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006* – *Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU - Notification from Denmark*, 8913/19, Brussels, 29 April 2019.

- Council of the EU, *Schengen Information System applications for EUROJUST*, 13389/02, Brussels, 22 October 2002.
- Council of the EU, *Second Annual Report of Eurojust (Calendar Year 2003)*, 8284/1/04 REV 1, Brussels, 26 April 2004.
- Council of the EU, *Second annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit*, 10464/05, Brussels, 23 June 2005.
- Council of the EU, *Setting of minimum age for recoding and storing facial images and fingerprints on the chip of a passport or residence and in the Visa Information System*, 9403/06, Brussels, 23 May 2006.
- Council of the EU, *Signature of a protocol on Denmark's participation in the Dublin/Eurodac agreement with Switzerland and Liechtenstein*, 7059/08, Brussels, 28 February 2008.
- Council of the EU, *Statement by Federal Minister Schily at the informal Council in Marseilles on 28 and 29 July 2000 on the development of police cooperation and the Schengen Information System*, 10959/00, Brussels, 31 August 2000.
- Council of the EU, *Strategic Seminar Eurojust: New Perspectives in Judicial Cooperation Budapest, 15-17 May 2011 Report*, 14428/11, Brussels, 21 September 2011.
- Council of the EU, *Strengthening the European external borders agency Frontex - Political agreement between Council and Parliament*, 11916/11, Brussels, 23 June 2011.
- Council of the EU, *Structure and main principles of the roadmap for standardisation for data quality purposes - Presidency discussion paper*, 7125/20, Brussels, 15 April 2020.
- Council of the EU, *Subject: Draft Charter of Fundamental Rights of the European Union— Amendments submitted by the members of the Convention regarding civil and political rights and citizens' rights (Reference document: CHARTE 4284/00 CONVENT 28 (REV 1 in French only), (oR. multilingual), CHARTE 4332/00, CoNVENT 35*, Brussels, 25 May 2000.
- Council of the EU, *Submission of the 2011 Activity Report of the Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 12913/12, Brussels, 25 July 2012.
- Council of the EU, *Submission of the Work Programmes 2012 and 2013 of the Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, 6401/13, Brussels, 28 February 2013.

- Council of the EU, *Summary Note on the Impact assessment for the Inclusion of Passport Copies (and other scanned documents) to Eurodac*, 7694/17, Brussels, 27 March 2017.

- Council of the EU, *Summary of the 38th meeting of the Eurodac Advisory Group, Summary of the 38th meeting of the Eurodac Advisory Group*, 13879/21, Brussels, 12 November 2021.

- Council of the EU, *The Stockholm Programme – An open and secure Europe serving and protecting the citizens*, 17024/09, Brussels, 2 December 2009.

- Council of the EU, *Third round of Mutual Evaluations "Exchange of information and intelligence between Europol and the Member States and among the Member States respectively"*, 9501/04, Brussels, 9 June 2004.

- Council of the EU, *Transfer of personal data to third parties: Article 48 of the Council Decision on the establishment, operation and use of the second generation Schengen Information System (SIS II)*, 14092/05, Brussels, 9 December 2005.

- Council of the EU, *Universal Message Format (UMF) 3 Proposal for the 5th IMS action list*, 6882/16, Brussels, 10 March 2016.

- Council of the EU, *Use and optimisation of Interpol instruments to identify and find missing persons*, 6980/16, Brussels, 11 March 2016.

- Council of the EU, *Use of images of the iFADO database for Frontex Quick Check Cards*, 7819/16, Brussels, 28 April 2016.

- Council of the EU, *VIS Regulation in the Commission Staff Working Document Evaluation of the implementation of Regulation (EC) No 767/2008 of the European Parliament and Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) / REFIT Evaluation Accompanying the document Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the Visa Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation*, 13530/16 ADD 2, Brussels, 21 October 2016.

- Council of the EU's documents, *Fingerprinting of illegal immigrants: Feasibility study of the possible extension of the Eurodac Convention*, 7566/98, Brussels, 8 April 1998.

- Council of the UE, *Comments on the recommendation for a Council decision authorising the opening of negotiations on the modernisation of Council of Europe Convention for the protection of individuals with regard to automatic processing of personal*

data (EST 108) and the conditions and modalities of accession of the European Union to the modernised Convention, 6655/13 EXT 1 (18.03.2013), Brussels, 20 February 2013.

- Council of the UE, *Conclusions of the European Council meeting*, EUCO 34/16, Brussels, 15 December 2016.

- Council of the UE, *European Council meeting (17 and 18 December 2015) – Conclusions*, EUCO 28/15, Brussels, 18 December 2015.

- Council of the UE, *Frontex Annual Risk Analysis 2021: The Cross-Border Crime dimension with the angle of the external borders*, 7233/21, Brussels, 25 March 2021.

- Council of the UE, *Frontex General Report 2007*, 17441/08, Brussels, 18 December 2008.

- Council of the UE, *Note from the Presidency, List of third States and organizations with which Europol shall conclude agreements*, 6473/14, Brussels, 17 February 2014.

- Council of the UE, *Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European criminal records information system (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011 - Revised text following COPEN meeting on 11 and 12 September 2017*, 12187/17, Brussels, 19 September 2017.

- Declaration No 17 on Article 73k of the Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, *OJC* 340, 10.11.1997, pp. 1-144.

- European Commission Communication, *Interoperability for Pan-European e-Government Services*, COM(2006) 45 final, Brussels, 13 February 2006.

- European Commission Proposal for a Council Decision authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, COM(2021) 719 final, Brussels, 25.11.2021.

- European Commission, *2014 Report on the Application of the EU Charter of Fundamental Rights*, COM(2015) 191, Brussels, 8.05.2015.

- European Commission, *Feasibility study on a Common Identity Repository (CIR)*, Brussels, 2017.

- European Commission, *New European Interoperability Framework: Promoting seamless services and data flows for European public administrations*, Brussels, 2017.

- European Commission, Vademecum on the external action of the European union, SEC(2011) 881/3, Brussels, 21.11.2012.

- European Council, The Hague Programme: strengthening freedom, security and justice in the European Union, *OJ C* 53, 3.3.2005, pp. 1-14.

- European Parliament legislative resolution of 13 March 2019 on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA, COM(2018) 0302, Brussels, 13.03.2019.

- European Parliament resolution of 12 February 2020 on automated decision-making processes: ensuring consumer protection and free movement of goods and services (2019/2915(RSP)), *OJ C* 294, 23.7.2021, pp. 14-17.

- European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)), *OJ C* 378, 9.11.2017, pp. 10-135.

- European Parliament resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance (2013/2831(RSP)), *OJ C* 208, 10.6.2016, pp. 153-156.

- European Parliament, *Interoperability between EU border and security information systems*, Brussels, 2019.

- European Parliament, *Interoperability between EU information systems for security, border and migration management*, PE 628.267, 2019.

- European Parliament, *Objection to a delegated act: Determining cases where identity data may be considered as same or similar for the purpose of the multiple identity detection pursuant to Regulation (EU) 2019/817*, P9_TA(2022)0007, Strasbourg, 20 January 2022.

- Explanations relating to the Charter of Fundamental Rights, *OJ C* 303, 14.12.2007, pp. 17-35.

- Explanatory Memorandum of the Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of Regulation (EU) XXX/XXX [Regulation on Asylum and Migration Management] and of Regulation (EU) XXX/XXX [Resettlement Regulation], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement

authorities and Europol for law enforcement purposes and amending Regulations (EU) 2018/1240 and (EU) 2019/818, COM(2020) 614 final, Brussels, 23.9.2020.

- Green Paper on detection technologies in the work of law enforcement, customs and other security authorities, COM(2006) 474 final, Brussels, 1.9.2006.

- Green Paper on the future Common European Asylum System, COM(2007) 301 final, Brussels, 6.6.2007.

- Interoperability solutions for European public administrations (ISA), *OJ L* 260, 3.10.2009, p. 20.

- Joint Statement by the Council and the Representatives of the Governments of the Member States meeting within the Council, the European Parliament and the European Commission, *THE EUROPEAN CONSENSUS ON HUMANITARIAN AID. The humanitarian challenge*, *OJ C* 25, 30.1.2008, pp. 1-12.

- List of proposals pending before the Council on 31 October 1993 for which entry into force of the Treaty on European Union will require a change in the legal base and/or a change in procedure, COM(93) 570 final, Brussels, 10.11.1993.

- Opinion of the Commission pursuant to Article 189b(2)(d) of the EC Treaty, on the European Parliament' s amendments to the Council' s common position regarding the proposal for a European Parliament and Council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(95) 0375 final, Brussels, 18.07.1995.

- Presidency Conclusions European Council meeting in Laeken 14 and 15 December 2001, DOC/01/18.

- Proposal for a Council Decision on the conclusion of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, COM(2013)0528 final, Brussels, 18.07.2013.

- Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM(90) 314 final, *OJ C* 277, 5.11.1990.

- Proposal for a Council framework decision on the exchange of information under the principle of availability, COM(2005) 0490 final, Brussels, 12.10.2005.

- Proposal for a Council Regulation on the establishment and operation of an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing Regulation (EU) No 1053/2013, COM(2021) 278 final, Brussels, 2.6.2021.

- Proposal for a Directive of the European Parliament and of the Council amending Council Decision 2005/671/JHA, as regards its alignment with Union rules on the protection of personal data, COM(2021) 767 final, Brussels, 1.12.2021.

- Proposal for a Directive of the European Parliament and of the Council on common standards and procedures in Member States for returning illegally staying third-country nationals (recast). A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018, COM(2018) 634 final, Brussels, 12.09.2018.

- Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, Brussels, 25.1.2012.

- Proposal for a Directive of the European Parliament and of the Council on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA, COM(2021) 782 final, Brussels, 8.12.2021, pp. 2-3.

- Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2018/1727 of the European Parliament and the Council and Council Decision 2005/671/JHA, as regards the digital information exchange in terrorism cases, COM(2021) 757 final, Brussels, 1.12.2021.

- Proposal for a Regulation of the European Parliament and of the Council establishing a collaboration platform to support the functioning of Joint Investigation Teams and amending Regulation (EU) 2018/1726, COM(2021) 756 final, Brussels, 1.12.2021

- Proposal for a Regulation of the European Parliament and of the Council on the European Border and Coast Guard and repealing Council Joint Action No 98/700/JHA, Regulation (EU) No 1052/2013 of the European Parliament and of the Council and Regulation (EU) No 2016/1624 of the European Parliament and of the Council A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018, COM(2018) 631 final, Brussels, 12.9.2018.

- Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol, COM(2020) 791 final, Brussels, 9.12.2020.

- Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA, COM(2018) 302 final, Brussels, 16.5.2018.

- Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM(2021) 281 final, Brussels, 3.6.2021.

- Proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (Recast version), COM(2008) 825 final, Brussels, 4.5.2016.

- Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JAI, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, COM(2017) 0793 final, Brussels, 13.12.2017.

- Proposal for a Regulation of the European Parliament and of the Council on the establishment of a framework for the interoperability of EU information systems (police and judicial cooperation, asylum and migration), COM(2017) 0794 final, Brussels, 13.12.2017.

- Proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011, COM(2017) 352 final, Brussels, 29.6.2017.

- Proposal for a Regulation of the European Parliament and of the Council on a computerised system for communication in cross-border civil and criminal proceedings (e-CODEX system), and amending Regulation (EU) 2018/1726, COM(2020) 712 final, Brussels, 2.12.2020.

- Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, COM(2009) 292 final, COM(2009) 294 final, Brussels, 24.6.2009.

- Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No. 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624, 2016/0357 (COD), COM(2016) 731 final, Brussels, 16.11.2016.

- Proposal for a Regulation of the European Parliament and of the Council establishing the conditions for accessing other EU information systems for ETIAS purposes and amending Regulation (EU) 2018/1240, Regulation (EC) No 767/2008, Regulation (EU) 2017/2226 and Regulation (EU) 2018/1861, COM(2019) 4 final, Brussels, 7.1.2019.

- Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System, COM(2016) 0196 final, Brussels, 6.4.2016.

- Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011, COM(2016) 0194 final, Brussels, 6.4.2016.

- Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562(2006) as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP), COM(2013) 96 final, Brussels, 28.02.2013.

- Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union, COM(2013) 95 final, Brussels, 28.02.2013.

- Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA, COM(2018) 302 final, Brussels, 16.5.2018.

- Proposal for a Regulation of the European Parliament and of the Council introducing a screening of third country nationals at the external borders and amending Regulations (EC) No. 767/2008, (EU) 2017/2226, (EU) 2018/1240 and (EU) 2019/817, COM(2020) 612 final, Brussels, 23.9.2020.

- Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] , for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast), COM(2016) 272 final, Brussels, 4.5.2016.

- Proposal for a Regulation of the European Parliament and of the Council on asylum and migration management and amending Council Directive (EC) 2003/109 and the proposed Regulation (EU) XXX/XXX [Asylum and Migration Fund], COM(2020) 610 final, Brussels, 23.9.2020.

- Proposal for a Regulation of the European Parliament and of the Council establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast), COM(2016) 0270 final, Brussels, 4.5.2016.

- Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation, COM(2020) 796 final, Brussels, 9.12.2020.

- Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006, COM(2016) 0882 final, Brussels, 21.12.2016.

- Proposal for a Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third-country nationals, COM(2016) 0881 final, Brussels, 21.12.2016.

- Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM(2021) 206 final, Brussels, 21.4.2021.

- Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 011 final, Brussels, 25.01.2012.

- Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA, COM(2018) 302 final, Brussels, 16.5.2018.

- Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast), COM(2016) 0272 final, Brussels, 4.5.2016.

- Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council, COM(2021) 784 final, Brussels, 8.12.2021.

- Proposal for a Regulation of the European Parliament and the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations, (EU) No. 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624, COM(2016) 0731 final, Brussels, 16.11.2016.

- Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2018/1727 of the European Parliament and the Council, as regards the collection, preservation and analysis of evidence relating to genocide, crimes against humanity and war crimes at Eurojust, COM(2022) 187 final, Brussels, 25.4.2022.

- Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the Hashemite Kingdom of Jordan on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Jordanian competent authorities for fighting serious crime and terrorism, COM(2017) 798 final, Brussels, 20.12.2017.

- Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the Republic of Turkey on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation

(Europol) and the Turkish competent authorities for fighting serious crime and terrorism, COM(2017) 799 final, Brussels, 30.10.2019.

- Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the Lebanese Republic on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Lebanese competent authorities for fighting serious crime and terrorism, COM(2017) 805 final, Brussels, 20.12.2017.

- Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the State of Israel on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Israeli competent authorities for fighting serious crime and terrorism, COM(2017) 806 final, Brussels, 19.12.2018.

- Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and Tunisia on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Tunisian competent authorities for fighting serious crime and terrorism, COM(2017) 807 final, Brussels, 21.12.2017.

- Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the Kingdom of Morocco on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Moroccan competent authorities for fighting serious crime and terrorism, COM(2017) 808 final, Brussels, 20.12.2017.

- Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the Arab Republic of Egypt on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Egyptian competent authorities for fighting serious crime and terrorism, COM(2017) 809 final, Brussels, 20.12.2017.

- Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the People's Democratic Republic of Algeria on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Algerian competent authorities for fighting serious crime and terrorism, COM(2017) 811 final, Brussels, 21.12.2017.

- Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals, PE/34/2018/REV/1, *OJ L* 312, 7.12.2018, pp. 1-13.

- Report from the Commission to the European Parliament and the Council concerning the exchange through the European Criminal Records Information System (ECRIS) of information extracted from criminal records between the Member States COM(2020) 778 final, Brussels, 29.6.2017.

- Report from the Commission to the European Parliament and the Council concerning the exchange through the European Criminal Records Information System (ECRIS) of information extracted from criminal records between the Member States, COM(2017) 0341 final, Brussels, 29.6.2017.

- Report from the Commission to the European Parliament and the Council on the state of play of preparations for the full implementation of the new legal bases for the Schengen Information System (SIS) in accordance with Article 66(4) of Regulation (EU) 2018/1861 and Article 79(4) of Regulation (EU) 2018/1862, COM(2021) 336 final, Brussels, 29.6.2021.

- Report of the Council of the EU, *The future of EU migration and asylum policy — Outcome of discussions*, 14364/19, Brussels, 22 November 2019.

- Roadmap, Border and law enforcement - advance air passenger information (API) - revised rules, and the attached Inception Impact Assessment, available at www.ec.europa.eu.

- Statement of the President of the European Commission Jean-Claude Juncker on the State of the Union of 14 September 2016, available at www.ec.europa.eu.

- Updated European Union Guidelines on promoting compliance with international humanitarian law (IHL), *OJ C* 303, 15.12.2009, pp. 12-17.

Organs and bodies

- Article 29 DPWP, *Adequacy Referential*, Brussels, 6.02.2018.

- Article 29 DPWP, *Mandate to the Enforcement Subgroup to proceed to the 2nd joint investigation action*, Brussels, 17.07.2008.

- Article 29 DPWP, *Second Annual Report*, Brussels, 30.11.1998.

- Article 29 DPWP, *Strategy Document*, Brussels, 29.09.2004.

- Article 29 DPWP, *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, Brussels, 1.12.2009.

- Article 29 DPWP, *Third Annual Report*, Brussels, 22.12.2000.

- Article 29 DPWP, *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, Brussels, 07.1998.
- Assessment of the EDPS on *the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, Brussels, 11.04.2017.
- Comments of the EDPS on *the Communication of the Commission on interoperability of European databases*, Brussels, 10.03.2006.
- Comments of the EDPS on *the Communication of the Commission on interoperability of European databases*, Brussels, 10.05.2006.
- Comments of the EDPS on *the model for working arrangements to be concluded by the European Border and Coast Guard Agency with the authorities of third countries*, Brussels, 3.07.2020.
- Work Programme of the EDPB No. 2021/2022, Brussels, 16.03.2021.
- Consultation of the EDPS on *the future EU-US international agreement on personal data protection and information sharing for law enforcement purposes*, Brussels, 12.03.2013.
- Corte dei Conti Europea, “Le Agenzie dell’Unione Europea: ottenere risultati”, *Relazioni Speciali*, No. 5, 2008.
- Court of Auditors, *EU readmission cooperation with third countries: relevant actions yielded limited results*, Luxembourg, 2021.
- Court of Auditors, *Europol support to fight migrant smuggling: a valued partner, but insufficient use of data sources and result measurement*, Luxembourg, 2021.
- Discussion Document of the Article 29 DPWP, *First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy*, Brussels, 26.06.1997.
- Document of the DG Migration and Home Affairs, *Special Eurobarometer 464b: Europeans’ towards security*, TNS opinion and political Wave EB87.4, Brussels, 2017.
- EBCG Agency, *Risk Analysis for 2019*, 1218/2019, Warsaw, 2019.
- EDPB No. 2/2018 on *derogations of Article 49 under Regulation 2016/679*, Brussels, 25.05.2018.
- EDPB, “Thirtieth Plenary session: EDPB response to NGOs on Hungarian Decrees and statement on Article 23 GDPR”, *Press Release*, Brussels, 3.06.2020.
- EDPB, “Thirty-second plenary session: Statement on the interoperability of contact tracing applications, statement on the opening of borders and data protection rights, response

letters to MEP Körner on laptop camera covers and encryption and letter to the Commission”, *Press Release*, Brussels, 17.06.2020.

- EDPB, *Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities*, Brussels, 5.08.2021.

- EDPB, *Toolbox on essential data protection safeguards for enforcement cooperation between EEA data protection authorities and competent data protection authorities of third countries*, Brussels, 14.03.2022.

- Decision of the EDPS concerning *the investigation into Frontex’s move to the Cloud*, Brussels, 1.04.2022.

- Decision of the EDPS on *the retention by Europol of datasets lacking Data Subject Categorisation*, Brussels, 21.12.2021.

- EDPS on *the Commission Implementing Decisions laying down the performance requirements and practical arrangements for monitoring the performance of the shared Biometric Matching Service pursuant to Regulation (EU) 2019/817 and Regulation (EU) 2019/818 of the European Parliament and of the Council*, Brussels, 31.03.2021.

- EDPS on *the draft Commission Implementing Decisions on: 1. the minimum data quality standards and technical specifications for biometric data in the Schengen Information System (SIS) in the field of border checks and return 2. the minimum data quality standards and technical specifications for biometric data in the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters*, Brussels, 26.08.2020.

- EDPS on *the proposal for a Council Regulation amending Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban, (2009/C 276/01)*, Brussels, 17.11.2009.

- EDPS on *various legislative proposals imposing certain specific restrictive measures in respect of Somalia, Zimbabwe, the Democratic Republic of Korea and Guinea, (2010/C 73/01)*, Brussels, 23.3.2010.

- EDPS, *Annual Report*, Brussels, 2021.

- EDPS, *Contribution of the EDPS to the consultation on the future EU-US international agreement on personal data protection and information sharing for law enforcement purposes*, Brussels, 12.03.2010.

- EDPS, *Monitoring and Ensuring Compliance with Regulation (EC) 45/2001. Policy Paper*, Brussels, 13.12.2010.
- EDPS, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, Brussels, 26.03.2014.
- eu-LISA *Feasibility Study – final report*, Tallin, 2018.
- eu-LISA, *Consolidated Annual Activity Report 2020*, Tallin, 29.06.2021.
- eu-LISA, *Elaboration of a Future Architecture for Interoperable IT Systems at eu-LISA*, Tallin, 2019.
- eu-LISA, *Report on the technical functioning of Central SIS II and the Communication Infrastructure, including the security thereof and the bilateral and multilateral exchange of supplementary information between Member States*, Tallin, 2015.
- eu-LISA, *Shared Biometric Matching Service (sBMS), Feasibility Study - final report*, Tallin, 2018.
- eu-LISA's report on *Smart Borders Pilot Project. Report on the technical conclusions of the Pilot*, Tallin, 2015.
- European Court of Auditors, *Lessons from the European Commission's development of the second generation Schengen Information System (SIS II)*, Luxembourg, 2014.
- European Migrant Smuggling Center, *4TH ANNUAL ACTIVITY REPORT – 2020*, The Hague, 2020.
- European Ombudsman, *Decision in case 1276/2018/FP on the European Commission's alleged failure to disclose the names of the national authorities participating in the High-Level Expert Group on Information System and Interoperability*, Strasbourg, 20 March 2019.
- Europol, *Facing Reality? Law enforcement and the challenge of deepfakes*, Luxembourg, 2022.
- Europol, *Integration of Europol into shared Biometric Matching System (sBMS)*, Ref. Ares(2020)3392333, 29.06.2020.
- Formal comments of the EDPS on *the draft Commission Delegated Regulations supplementing Regulation (EU) 2019/97 and Regulation (EU) 2019/818 of the European Parliament and Council with regard to cases where identity data may be considered as same or similar for the purpose of the multiple identity detection*, Brussels, 27.04.2021.
- Formal comments of the EDPS on *the draft Commission Implementing Regulations laying down the details of the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum quality standards for storage of data*

pursuant to Article 37(4) of Regulation (EU) 2019/817 and Article 37(4) of Regulation (EU) 2019/818 of the European Parliament and of the Council, Brussels, 30.04.2021.

- Formal comments of the EDPS on the draft Commission Implementing Decision laying down the specifications for technical solutions to manage user access requests for the purposes of Article 22 of Regulation (EU) 2019/817 and to facilitate the collection of the information for the purpose of generating reports, pursuant to Article 78(10) of Regulation (EU) 2019/817 of the European Parliament and of the Council, as well as on the draft Commission Implementing Decision laying down the specifications for technical solutions to manage user access requests for the purposes of Article 22 of Regulation (EU) 2019/818 and to facilitate the collection of the information for the purpose of generating reports, pursuant to Article 74(10) of Regulation (EU) 2019/818 of the European Parliament, Brussels, 27.09.2021.

- Formal comments of the EDPS on the draft Commission Implementing Decisions laying down a standard form for notification of a white link pursuant to Regulation (EU) 2019/817 and Regulation (EU) 2019/818 of the European Parliament and of the Council, Brussels, 22.04.2021.

- Formal comments of the EDPS on the draft Commission Implementing Decision laying down standard for refusal, annulment or revocation of a travel authorisation pursuant to Article 38(3) of Regulation (EU) 2018/1240, Brussels, 25.05.2021.

- Formal comments of the EDPS on the draft Commission Implementing Decisions laying down the technical rules for creating links between data from different EU information systems pursuant to Article 28(7) of Regulation (EU) 2019/817 and Article 28(7) of Regulation (EU) 2019/818 of the European Parliament and of the Council, Brussels, 17.04.2021.

- Formal comments of the EDPS on the draft Commission Implementing Decisions specifying the technical procedure for the European search portal to query the EU information systems, Europol data and Interpol databases and the format of the European search portal's replies, pursuant to Article 9(7) of Regulation (EU) 2019/817 of the European Parliament and of the Council, Brussels, 17.05.2021.

- Formal comments of the EDPS on the draft Commission Implementing Decisions on: 1. the minimum data quality standards and technical specifications for biometric data in the Schengen Information System (SIS) in the field of border checks and return 2. the minimum data quality standards and technical specifications for biometric data in the Schengen

Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, Brussels, 26.08.2020.

- Formal comments of the EU on *the draft Commission Implementing Decision laying down a standard form for notification of a red link pursuant to Regulation (EU) 2019/817 of the European Parliament and the Council*, Brussels, 31.03.2021.

- FRA, *Fundamental rights and the interoperability of EU information systems: borders and security*, Vienna, 2017.

- FRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Vienna, 2018.

- Guidelines of the Article 29 DPWP No. 4/2019 on *Article 25 Data Protection by Design and by Default Version 2.0*, Brussels, 20.10.2020.

- Guidelines of the Article 29 DPWP on *Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679*, Brussels, 4.04.2017.

- Guidelines of the Article 29 DPWP on *Data Protection Officers ('DPOs')*, Brussels, 13.12.2016.

- Guidelines of the Article 29 DPWP on *Data Protection Officers ('DPOs')*, Brussels, 13.12.2017.

- Guidelines of the EDPB No. 05/2021 on *the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, Brussels, 18.11.2021.

- Guidelines of the EDPB No. 10/2020 on *restrictions under Article 23 GDPR. Version 1.0*, Brussels, 15.12.2020.

- Guidelines of the EDPB No. 2/2020 on *articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies*, Brussels, 15.12.2020.

- High-Level Expert Group on information systems and interoperability, *Final Report*, Ares(2017)2412067, Brussels, 11 May 2017.

- Joint contribution of the Article 29 DPWP on *the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, Brussels, 1.12.2009.

- Joint Declaration of the European Parliament, the Council of the European Union and the European Commission, *EU Legislative Priorities for 2022*, Brussels, 2022.

- Joint Opinion of the EDPB-EDPS No. 04/2021 on *the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate)*, Brussels, 31.03.2021.

- Joint Opinion of the EDPB-EDPS No. 5/2021 on *the proposal for a Regulation of the European parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act)*, Brussels, 18.06.2021.

- Joint Opinion of the EDPS-EDPB No. 2/2021 on *the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries for the matters referred to in Article 46(2)(c) of Regulation (EU) 2016/679*, Brussels, 14.01.2021.

- Joint Opinion of the EDPS-EDPB on *eHDSI*, Brussels, 12.07.2019.

- Joint Research Centre Technical Report, *AI Watch: Beyond pilots: sustainable implementation of AI in public services*, Luxembourg, 2021.

- Letter of the Chair of the EDPB to Chairman of the Committee on Civil Liberties, Justice and Home Affairs, Brussels, 22.02.2022.

- Letter of the EDPB to the European Parliament, Brussels, 7.06.2021.

- Letter of the EDPS on *three legislative proposals concerning certain restrictive measures*, Brussels, 20.07.2010.

- Opinion of the EDPS No. 1/99 on *the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government*, Brussels, 26.01.1999.

- Opinion of the EDPS No. 2/99 on *the Adequacy of the "International Safe Harbor Principles" issued by the US Department of Commerce*, Brussels, 19.04.1999.

- Opinion of the EDPS No. 3/2018, *EDPS Opinion on online manipulation and personal data*, Brussels, 1.03.2018.

- Opinion of the EDPS No. 4/2000 on *the level of protection provided by the "Safe Harbor Principles"*, Brussels, 16.05.2000.

- Opinion of EDPS on *the Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries*, Brussels, 19.10.2010.

- Opinion of the Article 29 DPWP No. 1/2001 on *the Draft Commission Decision on Standard Contractual Clauses for the transfer of Personal Data to third countries under Article 26(4) of Directive 95/46*, Brussels, 26.01.2001.

- Opinion of the Article 29 DPWP No. 01/2012 on *the data protection reform proposals*, Brussels, 23.03.2012.
- Opinion of the Article 29 DPWP No. 01/2013 *providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive*, Brussels, 26.02.2013.
- Opinion of the Article 29 DPWP No. 1/2009 on *pre-trial discovery for cross border civil litigation*, Brussels, 11.02.2009.
- Opinion of the Article 29 DPWP No. 04/2014 on *Surveillance of electronic communications for intelligence and national security purposes*, Brussels, 10.04.2014.
- Opinion of the Article 29 DPWP No. 01/2014 on *the "Application of necessity and proportionality concepts and data protection within the law enforcement sector"*, Brussels, 27.02.2014.
- Opinion of the Article 29 DPWP No. 02/2012 on *facial recognition in online and mobile services*, Brussels, 22.03.2012.
- Opinion of the Article 29 DPWP No. 03/2013 on *purpose limitation*, Brussels, 2.04.2013.
- Opinion of the Article 29 DPWP No. 1/2010 on *the concepts of "controller" and "processor"*, Brussels, 16.02.2010.
- Opinion of the Article 29 DPWP No. 10/2004 on *More Harmonised Information Provisions*, Brussels, 25.11.2004.
- Opinion of the Article 29 DPWP No. 10/2006 on *the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, Brussels, 22.11.2006.
- Opinion of the Article 29 DPWP No. 3/2010 on *the principle of accountability*, Brussels, 13.07.2010.
- Opinion of the Article 29 DPWP No. 4/2003 on *the Level of Protection ensured in the US for the Transfer of Passengers' Data*, Brussels, 13.06.2003.
- Opinion of the Article 29 DPWP No. 4/2005 on *the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005)*, Brussels, 21.10.2005.
- Opinion of the Article 29 DPWP No. 4/2007 on *the concept of personal data*, Brussels, 20.06.2007.

- Opinion of the Article 29 DPWP No. 5/2001 on *the European Ombudsman Special Report to the European Parliament following the draft recommendation to the European Commission in complaint 713/98/IJH*, Brussels, 17.05.2001.

- Opinion of the Article 29 DPWP No. 5/2002 on *the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data*, Brussels, 11.10.2002.

- Opinion of the Article 29 DPWP on *Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration*, Brussels, 11.04.2018.

- Opinion of the Article DPWP No. 3/2005 on *Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member State*, Brussels, 30.09.2005.

- Opinion of the EDPB No. 32/2021 on *the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/769 on the adequate protection of personal data in the Republic of Korea. Version 1.0*, Brussels, 24.09.2021.

- Opinion of the EDPS No. 03/2015 on *the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, Brussels, 1.12.2015.

- Opinion of the EDPS No. 06/2016 on *the Second EU Smart Borders Package Recommendations on the revised Proposal to establish an Entry/Exit System*, Brussels, 21.09.2016.

- Opinion of the EDPS No. 07/2016 on *the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations)*, Brussels, 21.09.2016.

- Opinion of the EDPS No. 1/2020 on *the negotiating mandate to conclude an international agreement on the exchange of personal data between Europol and New Zealand law enforcement authorities*, Brussels, 31.01.2020.

- Opinion of the EDPS No. 1/2021 on *the Proposal for a Digital Services Act*, Brussels, 10.02.2021.

- Opinion of the EDPS No. 1/2022 on *the two Proposals for Council Decision authorizing Member States to sign and ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, Brussels, 20.01.2022.

- Opinion of the EDPS No. 10/2020 on *the negotiating mandate to conclude ten agreements allowing the exchange of data between Eurojust and the competent authorities for judicial cooperation in criminal matters in certain third countries*, Brussels, 17.12.2020.
- Opinion of the EDPS No. 10/2021 on the *Proposal for a Council Regulation on the establishment and operation of an evaluation and monitoring mechanism to verify the application of the Schengen acquis*, Brussels, 27.07.2021.
- Opinion of the EDPS No. 11/2017 on *the Proposal for a Regulation on ECRIS-TCN*, Brussels, 12.12.2017.
- Opinion of the EDPS No. 2/2018 on *eight negotiating mandates to conclude international agreements allowing the exchange of data between Europol and third countries*, Brussels, 14.03.2018.
- Opinion of the EDPS No. 2/2021 on *the Proposal for a Digital Markets Act*, Brussels, 10.02.2021.
- Opinion of the EDPS No. 3/2015, *Europe's big opportunity. EDPS recommendations on the EU's options for data protection reform*, Brussels, 27.07.2015.
- Opinion of the EDPS No. 3/2017 on *the Proposal for a European Travel Information and Authorisation System (ETIAS)*, Brussels, 6.03.2017.
- Opinion of the EDPS No. 4/2015, *Towards a new digital ethics. Data, Dignity and Technology*, Brussels, 11.09.2015.
- Opinion of the EDPS No. 4/2016 on *the EU-U.S. Privacy Shield draft adequacy decision*, Brussels, 30.05.2016.
- Opinion of the EDPS No. 4/2018 on *the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, Brussels, 18.04.2018.
- Opinion of the EDPS No. 5/2006 on *the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States*, Brussels, 14.06.2006.
- Opinion of the EDPS No. 6/2015, *A further step towards comprehensive EU data protection. EDPS recommendations on the Directive for data protection in the police and justice sectors*, Brussels, 28.10.2015.
- Opinion of the EDPS No. 7/2015, *Meeting the challenges of big data: A call for transparency, user control, data protection by design and accountability*, Brussels, 19.11.2015.

- Opinion of the EDPS No. 8/2017 on *the proposal for a Regulation establishing a single digital gateway and the 'once-only' principle*, Brussels, 1.08.2017.

- Opinion of the EDPS No. 8/2021 on *the Recommendation for a Council decision authorizing the opening of negotiations for a cooperation agreement between the EU and INTERPOL*, Brussels, 25.05.2021.

- Opinion of the EDPS on *a notification for Prior Checking received from the Data Protection Officer of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) concerning the "Collection of names and certain other relevant data of returnees for joint return operations (JRO)"*, Brussels, 26.04.2010.

- Opinion of the EDPS on *Promoting Trust in the Information Society by Fostering Data Protection and Privacy*, Brussels, 18.03.2018.

- Opinion of the EDPS on *the Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data (2008/49/EC)*, Brussels, 25.10.2008.

- Opinion of the EDPS on *the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"*, Brussels, 16.11.2012.

- Opinion of the EDPS on *the Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee towards a European e-Justice Strategy, OJ C 276/8*, Brussels, 6.6.2009.

- Opinion of the EDPS on *the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"*, Brussels, 14.01.2011.

- Opinion of the EDPS on *the Communication from the Commission to the European Parliament and the Council - "Overview of information management in the area of freedom, security and justice"*, Brussels, 30.09.2010.

- Opinion of the EDPS on *the Communication from the Commission to the European Parliament and the Council entitled 'Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM)*, Brussels, 29.04.2013.

- Opinion of the EDPS on *the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows" and on the Communication from the Commission to the European Parliament and the Council on "the*

Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU", Brussels, 20.02.2014.

- Opinion of the EDPS on *the data protection reform package*, Brussels, 7.03.2012.

- Opinion of the EDPS on *the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection*, Brussels, 6.06.2009.

- Opinion of the EDPS on *the Initiative of the Kingdom of Belgium, the Czech Republic, the Republic of Estonia, the Kingdom of Spain, the French Republic, the Italian Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Poland, the Portuguese Republic, the Republic of Slovenia, the Slovak Republic and the Kingdom of Sweden with a view to adopting a Council Decision concerning the strengthening of Eurojust and amending Decision 2002/187/JHA, (2008/C 310/01)*, Brussels, 5.12.2008.

- Opinion of the EDPS on *the initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the French Republic, the Italian Republic, the Republic of Hungary, the Republic of Poland, the Portuguese Republic, Romania, the Republic of Finland and the Kingdom of Sweden for a Directive of the European Parliament and of the Council on the European Protection Order, and - on the initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the Republic of Austria, the Republic of Slovenia and the Kingdom of Sweden for a Directive of the European Parliament and of the Council regarding the European Investigation Order in criminal matters*, Brussels, 5.10.2010.

- Opinion of the EDPS on *the package of legislative measures reforming Eurojust and setting up the European Public Prosecutor's Office ('EPPO')*, Brussels, 5.03.2014.

- Opinion of the EDPS on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability, COM(2005) 490 final, OJ C 116, 17.05.2006.

- Opinion of the EDPS on *the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005) 490 final), (2006/C 116/04)*, Brussels, 17.05.2006.

- Opinion of the EDPS on *the Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA*, Brussels, 31.05.2013.

- Opinion of the EDPS on *the Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011*, Brussels, 2.03.2021.

- Opinion of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council, COM(2008) 820 final, Brussels, 23.9.2009, pp. 1-5.

- Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, *OJ C 255*, 27.10.2007, pp. 1-12.

- Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on an area of freedom, security and justice serving the citizen, *OJ C 276/8*, 17.11.2009, pp. 8-20.

- Opinion of the European Data Protection Supervisor on the Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Slovenia, the Slovak Republic, the Italian Republic, the Republic of Finland, the Portuguese Republic, Romania and the Kingdom of Sweden, with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, *OJ C 169*, 21.7.2007, pp. 2-14.

- Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision establishing the European Police Office (Europol), COM(2006) 817 final, Brussels, 27.10.2007.

- Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...][establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], COM(2008) 825, Brussels, 20.02.2009.

- Opinion of the European Data Protection Supervisor on the proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United

States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (TFTP II), *OJ C 355*, 29.12.2010, pp. 10-15.

- Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision establishing the European Police Office (Europol), COM(2006) 817 final, *OJ C-357/1*, 30.12.2010.

- Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability, COM(2005) 490 final, *OJ C 116*, 17.5.2006, pp. 8-17.

- Opinion of the European Economic and Social Committee on 'Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation (EU) 2018/... (Interoperability Regulation) and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA' (COM(2018) 302 final), EESC 2018/03954, *OJ C 440*, 6.12.2018, pp. 154-157.

- Opinion of the European Economic and Social Committee on the 'Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System' (COM(2016) 196 final — 2016/0105 (COD)) and on the 'Proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011' (COM(2016) 194 final — 2016/0106 (COD)), *OJ C 487*, 28.12.2016, pp. 66-69.

- Opinion of the FRA No. 2/2017, *The impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorization System (ETIAS)*, Vienna, 30.06.2017.

- Position Paper of the EDPS, *The transfer of personal data to third countries and international organisations by EU institutions and bodies*, Brussels, 14.07.2014.

- Preliminary Comments of the EDPS on - *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Preparing the next steps in border management in the European Union"*, COM(2008) 69 final; - *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee*

of the Regions, “Examining the creation of a European Border Surveillance System (EUROSUR)”, COM(2008) 68 final; - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, “Report on the evaluation and future development of the FRONTEX Agency”, COM(2008) 67 final, Brussels, 3.03.2008.

- Preliminary Opinion of the EDPS No. 1/2016 on *the agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences*, Brussels, 12.02.2016.

- Preliminary Opinion of the EDPS No. 5/2018 on *privacy by design*, Brussels, 31.05.2018.

- Preliminary Opinion of the EDPS, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, Brussels, 10.03.2014.

- Recommendation of the Article 29 DPWP No. 1/2000 on *the Implementation of Directive 95/46/EC*, Brussels, 3.02.2000.

- Recommendation of the Article 29 DPWP No. 1/99, Brussels, 23.02.1999.

- Recommendation of the Article 29 DPWP No. 4/99 on *the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights*, Brussels, 7.09.1999.

- Recommendation of the EDPB No. 02/2020 on *the European Essential Guarantees for surveillance measures*, Brussels, 10.11.2020.

- Recommendations of the EDPB No. 01/2020 on *measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data: Version 2.0*, Brussels, 18.06.2021.

- Recommendations of the EDPB No. 01/2021 on *the adequacy referential under the Law Enforcement Directive*, Brussels, 2.02.2021.

- Report from the Commission to the European Parliament and the Council, Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2008, COM(2009) 494 final, 25.9.2009.

- Report from the Commission to the European Parliament and the Council, Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2008, COM(2009) 13 final, 26.1.2009.

- Report from the Commission to the European Parliament and the Council, Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2008, COM(2010) 415 final, 3.08.2010.

- Report from the Commission to the European Parliament and the Council, Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2008, COM(2011) 549 final, 12.09.2011.

- Report from the Commission to the European Parliament and the Council, Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2008, COM(2012) 533 final, 21.09.2012.

- Report from the Commission to the European Parliament and the Council, Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2008, COM(2013) 485 final, 28.06.2013.

- Report of the Article 29 DPWP No. 1/2007 on *the first joint enforcement action: evaluation and future steps*, Brussels, 20.06.2007.

- Report of the Article 29 DPWP on *the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union*, Brussels, 18.01.2005.

- Second Opinion of the EDPS No. 5/2015 on *the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, Brussels, 24.09.2015.

- Second Opinion of the EDPS on *the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters*, Brussels, 26.04.2007.

- Second Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, *OJ C 91/9*, 24.4.2007.

- Statement of the Article 29 DPWP on *automatic inter-state exchanges of personal data for tax purpose*, Brussels, 4.02.2015.

- Statement of the Article 29 DPWP on *the role of a risk-based approach in data protection legal frameworks*, Brussels, 30.05.2014.

- Statement of the EDPS No. 04/2021 on *international agreements including transfers*, Brussels, 13.04.2021.

- Working Document of the Article 29 DPWP No. 01/2012 on *epSOS*, Brussels, 25.01.2012.

- Working Document of the Article 29 DPWP on *a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, Brussels, 25.11.2005.

- Working Document of the Article 29 DPWP on *E-Government*, Brussels, 8.05.2003.

- Working Document of the Article 29 DPWP on *surveillance of electronic communications for intelligence and national security purposes*, Brussels, 5.12.2014.

- Working Document of the Article 29 DPWP, *Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries*, Brussels, 22.04.1998.

- Working Document of the Article 29 DPWP, *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, Brussels, 07.1998.

- Working document on *the current state of play of the ongoing discussions between the European Commission and the United States Government concerning the "International Safe Harbor Principles"*, Brussels, 7.09.1999.

Others

- Asia-Pacific Economic Cooperation, *Privacy Framework*, Singapore, 2004.

- Association of Southeast Asian Nations, *Framework on Personal Data Protection*, Jakarta, 2016.

- ICRC, *Los migrantes desaparecidos y sus familiares: recomendaciones del CICR para los responsables de formular políticas*, Geneva, 2017.

- ICRC, *Policy on the Processing of Biometric Data by the ICRC*, Geneva, 2019.

- ICRC, *Rules on Personal Data Protection*, Geneva, 2020, and Id., *Policy on the Processing of Biometric Data by the ICRC*, Geneva, 2019.

- ICRC, *Rules on Personal Data Protection*, Geneva, 2020.

- IOM, *IOM Data Protection Manual*, Geneva, 2010.

- OECD, *Going Digital Toolkit: Interoperability of privacy and data protection frameworks*, Paris, 2021.

- OECD, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Paris, 1980.

- OECD, *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, Paris, 2007.

- Resolution of the International Conference of Data Protection and Privacy Commissioners on *Privacy and International Humanitarian Action*, Hong Kong, 26 September 201.

- UNHCR, *Guidance on the protection of personal data of persons of concern to UNHCR*, Geneva, 2018.

- UNHCR, *Handbook for registration. Procedures and Standards for Registration, Population Data Management and Documentation*, Geneva, 2003.

- White House, *Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy*, Washington D.C., 2012.

National

- Spanish Agency on Data Protection, *A Guide to Privacy by Design*, Madrid, 2019.

Annex

Table 1: Old generation of large-scale IT systems and Europol Information System - Source: Own elaboration

System	Legislation	Main purposes	Access rights	Data retention period	Personal data		
					Biometric data	Alphanumeric data	Travel /identity document data
SIS	<ul style="list-style-type: none"> Regulation (EC) No 1987/2006 for border management; Council Decision 2007/533/JHA for law enforcement cooperation, and Regulation (EC) No 1986/2006 for cooperation on vehicle registration 	The SIS ensure a high level of security within the AFSJ of the EU, including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States, and to apply the provisions relating to the movement of persons in their territories, using information communicated via this system according to Article 1(2) of Regulation (EC) No 1987/2006, and Article 1(2) of Council Decision 2007/533/JHA. The categories of alerts that can be entered into the SIS concern:	<ul style="list-style-type: none"> Article 27 of Regulation (EC) No 1987/2006 and Article 40 of Council Decision 2007/533/JHA refer to the authorities responsible for the identification of third-country nationals, namely border control, police, and customs. Moreover, judicial authorities can access the SIS for the initiation of public prosecutions in criminal proceedings and for judicial 	Article 29 of Regulation (EC) No 1987/2006 and Article 44 of Council Decision 2007/533/JHA set forth that alerts should be kept in the SIS for the time required to achieve the purposes for which they were entered. Member States must carry out periodic reviews: three years for all alert categories, except discreet or specific checks where the review period is one year.	Article 20(2)(e) and (f) of Regulation (EC) No 1987/2006, and Article 20(3)(e) and (f) of Council Decision 2007/533/JHA include: photographs, and fingerprints for both verification (one-to-one search) and identification (one-to-many search).	<p>Article 20(2) of Regulation (EC) No 1987/2006, and Article 20(3) of Council Decision 2007/533/JHA:</p> <p>1) Data for identifying the person or object, subject of the alert: surname(s), forename(s), name(s) at birth, previously used names and any aliases; any specific, objective, physical characteristics not subject to change; place and date of birth; sex; nationality(ies).</p> <p>2) A statement why the person or object is</p>	Article 38(2)(d) and (e) of Council Decision 2007/533/JHA: blank official documents which have been stolen, misappropriated or lost, and issued identity papers such as passports, identity cards, driving licenses, residence permits and travel documents which have been stolen, misappropriated, lost or invalidated.

System	Legislation	Main purposes	Access rights	Data retention period	Personal data		
		<ul style="list-style-type: none"> • refusal of entry or stay by virtue of Article 24 of Regulation (EC) No 1987/2006; • persons wanted for arrest for surrender or extradition purposes by virtue of Article 26 of Council Decision 2007/533/JHA); • missing persons by virtue of Article 32 of Council Decision 2007/533/JHA; • persons sought to assist with a judicial procedure according to Article 34 of Council Decision 2007/533/JHA; • persons and objects for discreet or specific checks by virtue of Article 36 of Council Decision 	<p>inquiries prior to charge; visa and migration authorities in the context of the application of the Community <i>acquis</i> relating to the movement of persons.</p> <ul style="list-style-type: none"> • Article 1 of Regulation (EC) No 1986/2006 adds the services in the Member States responsible for issuing registration certificates for vehicles. • Articles 41 and 42 states that Europol and Eurojust have access to the SIS but they cannot enter data in the SIS. • Article 40(8) of the 2016 EBCG Agency Regulation, the agency's teams have full 			<p>sought: reason for the alert; authority issuing the alert; a reference to the decision giving rise to the alert; link(s) to other alerts issued in SIS; the type of offence; whether the person concerned is armed, violent or has escaped.</p> <p>3) An instruction on the action to be taken when the person or object has been found.</p>	

System	Legislation	Main purposes	Access rights	Data retention period	Personal data		
		2007/533/JHA, and <ul style="list-style-type: none"> objects for seizure or use as evidence in criminal procedures by virtue of Article 38 of Council Decision 2007/533/JHA. 	access to the SIS to carry out searches.				
VIS	<ul style="list-style-type: none"> Regulation (EC) No 767/2008, and Council Decision 2008/633/JHA for law enforcement. 	<ul style="list-style-type: none"> Article 2 of the VIS Regulation establishes that the VIS has the purpose of improving the implementation of the common visa policy, consular cooperation and consultation between central visa authorities by facilitating the exchange of data between Member States on applications and on the decisions. 	<ul style="list-style-type: none"> Articles 6, and 18 to 22 of the VIS Regulation foresees: visa authorities; border authorities; immigration authorities, and asylum authorities. Article 1 of the VIS LEA Decision allows Member States' designated authorities and 	Article 23 of the VIS Regulation provides for a period of five years from the expiry of the visa or the refusal/annulment/revocation of the visa.	Article 5(1)(b) and (c) of the VIS Regulation gathers photographs scanned and ten fingerprints, with the exceptions made in its paragraph (2).	Article 5(1)(a) and (d) of the VIS Regulation include: surname and first name(s); date of birth; place/country of birth; sex; nationality; data on inviting person/organization; home address; current occupation and employer; minors: surname and first name of the applicant's parents; Member States of destination and first entry; main purpose of the journey, and intended date of	Article 9(4)(c) of the VIS Regulation foresees: type and number of travel document; issuing country; date of issue; date of expiry, and authority which issued the travel document.

System	Legislation	Main purposes	Access rights	Data retention period	Personal data		
		<ul style="list-style-type: none"> Article 1 of the VIS LEA Decision sets forth that Member States' designated authorities and Europol can consult the VIS for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences. 	Europol to access the VIS.			arrival and departure.	
Eurodac	Regulation (EU) No 603/2013	<p>Article 1 of the Eurodac Regulation provides that the system wants to:</p> <ul style="list-style-type: none"> assist in determining which Member State is to be responsible for examining an application for international protection, and lay down the conditions under which Member States' 	<p>Articles 14 to 22 of the Eurodac Regulation:</p> <ul style="list-style-type: none"> authorised users within the competent national authorities (asylum, police, border control authorities); Member States' designated authorities, and 	<ul style="list-style-type: none"> Article 12 of the Eurodac Regulation establishes a ten years period for asylum applicants, and Article 16 of the Eurodac Regulation foresees a maximum period of eighteen months of third country national apprehended while illegally crossing an external border. 	Article 11(a) of the Eurodac Regulation includes fingerprints.	Article 11(c) of the Eurodac Regulation includes sex.	

System	Legislation	Main purposes	Access rights	Data retention period	Personal data		
		designated authorities and the Europol may request the comparison of fingerprints.	<ul style="list-style-type: none"> Europol. 				
EIS	Regulation (EU) 2016/794	<p>Europol's information system stores information, including personal data, covering the crimes listed under Annex I to:</p> <ul style="list-style-type: none"> cross-checking aimed at identifying connections or other relevant links between information related to: persons who are suspected of having committed or taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence, and persons regarding whom 	<p>Articles 20, 21 25 of the Europol Regulation:</p> <ul style="list-style-type: none"> Europol's officials; Member State liaison officers; seconded national experts stationed at Europol headquarters; staff in the Europol National Units and competent authorities in the Member States; some of Europol's cooperation partners via Europol's operational centre; 	<p>Article 31 of the Europol Regulations provides for the storage of data as long as necessary and proportionate for the purposes for which the data are processed.</p> <p>Review of the need for continued storage no later than three years after the start of the initial processing of personal data. In case of continued storage of personal data, the following review takes place after another period of three years, if continued storage is still necessary. If no decision is taken on the continued storage of personal data, that data shall be erased automatically after three years.</p>	<p>Annex II to the Europol Regulation contemplates:</p> <ul style="list-style-type: none"> For the purposes of cross-checking: dactyloscopic data and DNA profiles of suspected persons. For the purposes of analyses of a strategic or thematic nature, for the purpose of operational analyses or for the purpose of facilitating the exchange of information: fingerprints; 	<p>Annex II to the Europol Regulation contemplates:</p> <ul style="list-style-type: none"> For the purposes of cross-checking: surname, maiden name, given names and any alias or assumed name; date and place of birth; nationality; sex; place of residence, profession and whereabouts of the person concerned, of suspected persons. For the purposes of cross-checking: criminal offences, alleged criminal offences and 	<p>Annex II to the Europol Regulation contemplates:</p> <ul style="list-style-type: none"> For the purposes of cross-checking: social security numbers, driving licences, identification documents of suspected persons. For the purposes of analyses of a strategic or thematic nature, for the purpose of operational analyses or for the purpose of facilitating

System	Legislation	Main purposes	Access rights	Data retention period	Personal data		
		<p>there are factual indications or reasonable grounds to believe that they will commit criminal offences in respect of which Europol is competent;</p> <ul style="list-style-type: none"> analyses of a strategic or thematic nature; operational analyses; facilitating the exchange of information between Member States, Europol, other Union bodies, third countries and international organisations. 	<ul style="list-style-type: none"> Eurojust, and OLAF. 		<p>DNA profile (established from the non-coding part of DNA), voice profile, blood group, dental information, video and photographic images.</p>	<p>when, where and how they were (allegedly) committed; means which were or which may have been used to commit those criminal offences, including information concerning legal persons; departments handling the case and their filing references; suspected membership of a criminal organisation; convictions, where they relate to criminal offences in respect of which Europol is competent, and inputting party.</p> <ul style="list-style-type: none"> For the purposes of analyses of a strategic or thematic nature, for the purpose of operational 	<p>the exchange of information: means of identification.</p>

System	Legislation	Main purposes	Access rights	Data retention period	Personal data		
						<p>analyses or for the purpose of facilitating the exchange of information;</p> <p>personal details; physical description; occupation and skills; economic and financial information; behavioral data; contacts and associates, including type and nature of the contact or association; means of communication used, such as telephone (static/mobile), fax, pager, electronic mail, postal addresses, internet connection(s); means of transport used, such as vehicles, boats, aircraft, including information identifying those means of</p>	

System	Legislation	Main purposes	Access rights	Data retention period	Personal data		
						transport (registration numbers); information relating to criminal conduct; references to other information systems in which information on the person is stored, and information on legal persons associated.	

Table 2: New generation of large-scale IT systems and Common Identity Repository - Source: Own elaboration

Forthcoming Database/ Component*	Legislation	Main purpose	Access rights	Data retention period	Personal data		
					Biometric data	Alphanumeric data	Travel /identity document data
SIS	Border management: Regulation (EU) 2018/1861, and Regulation (EU) 2018/1860 (return alerts). Law enforcement cooperation: Regulation (EU) 2018/1862.	New alert categories (additional): - Alerts on return (Article 3 of Regulation (EU) 2018/1860); - Preventive alerts (Children who need to be prevented from travelling; vulnerable persons who are of age who need to be prevented from travelling for their own protection) (Article 32 of Regulation (EU) 2018/1862); - Inquiry check (Article 36 of Regulation (EU) 2018/1862); - Alerts on unknown wanted persons for the	New (additional): - Registration services for boats and aircraft, and - Registration services for firearms (Regulation (EU) 2018/1862).	New maximum review periods: - 5 years for: alerts on persons wanted for arrest, and alerts on missing persons - 3 or 5 years depending on the underlying decision for: alerts on refusal of entry and stay, and alerts on return. - 3 years: alerts on persons sought to assist with a judicial procedure, and alerts on unknown wanted persons. - 1 year for: alerts on discreet, specific or inquiry	New (additional): - Latent fingerprints found at crime scenes; - DNA profiles (only for alerts on missing persons who need to be placed under protection, if additional conditions are fulfilled), and - Identification with photographs and facial images (several conditions, only after 2021).	New (additional): All alert categories: whether the person concerned has absconded, poses a risk of suicide, poses a threat to public health, and is involved in terrorist offences, offences related to a terrorist group, or to terrorist activities. Alerts under Regulation (EU) 2018/1862: registration number in a national register. Alerts for refusal of Regulation (EU) 2018/1861: whether the person is a family member of an EU citizen, and specification of the basis for the decision	New: - the category, the country of issue, the number(s), the date of issue of the person's identification documents, and - a copy of the identification documents, in colour wherever possible.

Forthcoming Database/ Component*	Legislation	Main purpose	Access rights	Data retention period	Personal data		
		<p>purpose of identification, and</p> <p>- Latent fingerprints found at crime scenes (Article 40 of Regulation (EU) 2018/1862).</p>		checks, and preventive alerts.		<p>for refusal of entry and stay.</p> <p>Alerts of Regulation (EU) 2018/1860: whether the return decision is issued in relation to a third-country national who poses a threat to public policy, to public security or to national security, and last date of the period for voluntary departure, if granted.</p> <p>Preventive alerts: categorisation of the type of case.</p>	
EES	Regulation (EU) 2017/2226	Recording and storage of date, time and place of entry and exit of third-country nationals crossing the borders of the Member States at which the EES is operated as well as storing data related to refusals of entry.	The below authorities/stakeholders have access to data stored in the EES. However, the extent of the access differs and the conditions for accessing the data differ. For some it is access right to enter/update data and have access to all the data stored, for others, it is limited to 'read-only' access, for others still to the status of whether a single or double entry visa has already been used by the traveler, for	<p>EES individual file and related entry/exit and refusal of entry records: 3 years.</p> <p>EES individual file and entry records without an exit record: 5 years.</p>	<p>Facial image.</p> <p>Four finger prints.</p>	<p>Surname (family name), first name or names (given names), date of birth, nationality, sex.</p> <p>Date and time of entry and exit.</p> <p>Data related to refusals of entry (date and time, border crossing point, authority that</p>	<p>Type, number and three letter code of the travel document(s).</p> <p>Date of expiry of the validity of travel document(s).</p>

Forthcoming Database/ Component*	Legislation	Main purpose	Access rights	Data retention period	Personal data		
		<p>Calculating the duration of authorised stay and generating alerts to Member States when the authorised stay has expired.</p> <p>Facilitating and assisting in the correct identification of persons in the EES under the conditions of Article 20 of the Interoperability Regulation.</p>	<p>others still it is subject to strict conditions.</p> <ul style="list-style-type: none"> - Border, visa and immigration authorities; - National authorities competent for Article 20 and 21 of the ‘Interoperability Regulations’; - Europol and national authorities designated for the purpose of the prevention, detection and investigation of terrorist offences or of other serious criminal offences, and - Carriers (only OK or NOT OK reply). 			<p>refused entry, reasons for refusing entry).</p> <p>Border crossing point of entry, authority that authorised entry.</p> <p>Status indicating whether family member without a residence permit.</p> <p>Data related to short stay visas.</p>	
ETIAS	Regulation (EU) 2018/1240	<p>To consider whether the presence of visa-exempt third country nationals in the territory of the Member States would pose a security, illegal immigration or high epidemic risk.</p> <p>Facilitating and assisting in the correct identification of persons in ETIAS</p>	<p>The below authorities/stakeholders have all access to data stored in ETIAS. However, the extent of the access differs and the conditions for accessing the data differ. For some it is full access to all the data stored, for others, it is limited to the status of a travel authorisation or is subject to strict conditions.</p>	<p>ETIAS application files:</p> <ul style="list-style-type: none"> - the period of validity of a travel authorisation (i.e., maximum of 3 years); - 5 years from the last decision to refuse, annul or 	N/A	<p>Surname (family name), first name or names (given names), surname at birth, date of birth, place of birth, sex, current nationality, country of birth, first names of the parents of the applicant, other names (if any), other nationalities (if any).</p>	<p>Type, number and country of issue of the travel document, date of issue</p> <p>The date of expiry of the travel document.</p>

Forthcoming Database/ Component*	Legislation	Main purpose	Access rights	Data retention period	Personal data		
		under the conditions of Article 20 of the Interoperability Regulation.	<ul style="list-style-type: none"> - Member State's ETIAS National Units; - ETIAS Central Unit established within Frontex; - Border authorities; - Immigration authorities; - National authorities competent for Article 20 and 21 of the 'Interoperability Regulations'; - Europol and national authorities designated for the purpose of the prevention, detection and investigation of terrorist offences or of other serious criminal offences, and - Carriers (only OK or NOT OK reply). 	revoke a travel authorisation.		<p>Applicants home address, email address (if available phone numbers), education, current occupation.</p> <p>Answers to a set of background questions (past criminal offences; stays in specific war or conflict zones; decisions requiring leaving the territory of Member States or the visa exempt third countries or any return decisions).</p> <p>For minors: identity data of legal guardian or parental authority.</p> <p>For persons benefitting from free movement without a residence permit: alphanumeric identity data of family members with whom the applicant has family ties with</p>	

Forthcoming Database/ Component*	Legislation	Main purpose	Access rights	Data retention period	Personal data		
VIS revised	Regulation (EU) 2021/1133 and Regulation (EU) 2021/1134	<p>Same as current VIS, but data on applicants for long-stay visas and residence permits will also be included.</p> <p>Additional access rights:</p> <ul style="list-style-type: none"> - Carriers (only OK or NOT OK), and - Frontex teams. 	<p>Same as current VIS.</p> <p>Additional access rights:</p> <ul style="list-style-type: none"> - Carriers (only OK or NOT OK), and - Frontex teams. 	<p>Same as current VIS (5 years), but earlier deletion of children's biometrics.</p> <p>EP also asks for deletion of data of persons having held residence for 10 years or more (still under negotiation).</p>	<p>10 fingerprints (except for children under 6 and some other cases).</p> <p>Live facial image.</p> <p>(biometrics collected for long-stay visas and residence permits depend on national rules).</p>	<p>Same as current VIS for short-stay visas.</p> <p>For long-stay visas/residence permits:</p> <ul style="list-style-type: none"> - Surname and first name(s); - Date of birth; - Place of birth; - Sex; - Nationality, and - Minors: surname and first name of the applicant's parents. 	<p>Same as current VIS, plus:</p> <p>Scan of the biographic data page of the travel document.</p>
Eurodac (forthcoming)	Based on the provisional agreement reached in 2018 and on the new Eurodac Amended Proposal	<p>Assist in determining which Member State is to be responsible pursuant to Regulation on Asylum and Migration Management;</p> <p>assist with the application of the Resettlement Regulation;</p>	<p>Authorised users within the competent national authorities (asylum, police, border control authorities);</p> <p>Member States' designated authorities, and</p> <p>Europol for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences.</p>	<p>Asylum applicants: 10 years.</p> <p>Resettled persons: 10 years.</p> <p>Irregular crossers of the external borders: 5 years.</p>	<p>Fingerprints and facial image</p>	<ul style="list-style-type: none"> - surname(s) and forename(s), name(s) at birth and previously used names and any aliases; - nationality(ies); - place and date of birth; 	Scanned colour copy of identity or travel document.

Forthcoming Database/ Component*	Legislation	Main purpose	Access rights	Data retention period	Personal data		
		<p>assist with the control of illegal irregular immigration to the Union and with the detection of secondary movements within the Union and with the identification of illegally staying third-country nationals and stateless persons;</p> <p>lay down the conditions under which Member States' designated authorities and Europol may request the comparison of biometric or alphanumeric data;</p> <p>assist in the correct identification of persons registered in Eurodac for the purposes of interoperability;</p> <p>support the objectives of ETIAS;</p> <p>support the objectives of VIS.</p>		<p>Illegally staying persons: 5 years.</p> <p>SAR persons: 5 years.</p>		<p>Sex, and</p> <p>- the type and number of identity or travel document, the three letter code of the issuing country and expiry date</p>	

Forthcoming Database/ Component*	Legislation	Main purpose	Access rights	Data retention period	Personal data		
ECRIS-TCN	Regulation (EU) 2019/816	Establishment of a system to identify the Member State(s) holding information on previous convictions of third-country nationals (ERIS-TCN) so that the criminal records information can be subsequently requested from those Member State(s) via existing European Criminal Records Information System (ECRIS).	Central authorities of the Member States designed in accordance with Art. 3(1) of Framework Decision 2009/315/JHA; Europol; Eurojust, and EPPO.	Each data record shall be stored in the central system for as long as the data related to the convictions of the person concerned are stored in the criminal records.	Fingerprint data, and Facial images	<ul style="list-style-type: none"> - Surname; - First names; - Date of birth; - Place of birth; - Nationalities; - Gender; - Previous names; - Parents' names; - Pseudonyms or aliases, and - Identity number. 	Type and number of the person's identification documents, as well as the name of the issuing authority.
Common Identity Repository (CIR)*	Regulation (EU) 2019/817 and Regulation (EU) 2019/817	Article 20 "Access to the common identity repository for identification"; Article 21 "Access to the common identity repository for the detection of multiple identities", and	Police authorities for identification; the authority responsible for the manual verification of different identities in order to resolve the yellow links, and designated authorities and Europol for the purposes of preventing, detecting or investigating terrorist offences	See the retention periods established by the underlying systems (i.e., EES, ETIAS, VIS, Eurodac and ECRIS-TCN). The Schengen Information System (SIS) is out of the CIR and so are the	Fingerprints and facial images according to the regulation of the underlying IT systems (i.e., EES, VIS, Eurodac and ECRIS-TCN).	Surname (family name); first name or names (given names); date of birth; place/country of birth;	Type and number of the travel document or documents; three letter code of the issuing country of the travel

Forthcoming Database/ Component*	Legislation	Main purpose	Access rights	Data retention period	Personal data		
		Article 22 “Querying the common identity repository for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences”.	or other serious criminal offences.	biographic data stored therein.		nationality or nationalities currently used and at birth, sex, and pseudonyms, artistic names, aliases, usual names, of the underlying large-scale IT systems (i.e., EES, ETIAS, VIS, Eurodac and ECRIS-TCN).	document or documents, and the date of expiry of the validity of the travel document or documents of the underlying IT systems (i.e., EES, ETIAS, VIS, Eurodac and ECRIS-TCN).

Table 3: Large-scale IT systems, main policy and ancillary purposes - Source: Own elaboration

System	Main policy area	Ancillary Purposes									
	TFEU	Article 77(2)(b) carrying out checks on persons and efficient monitoring of the crossing of external borders	Article 79(2)(c) illegal immigration and unauthorised residence, including removal and repatriation of persons residing without authorisation	Article 78 common policy on asylum	Article 77(2)(a) the common policy on visas and other short-stay residence permits	Article 77(2)(d) any measure necessary for the gradual establishment of an integrated management system for external borders	Article 77(2)(1)(e) the absence of any controls on persons when crossing internal borders	Article 87 police cooperation	Article 82 criminal judicial cooperation	Article 67	-
ETIAS	77(2)(b) and (d) and Article 87(2)(a)	- enhance the effectiveness of border checks, and - supports SIS alert on refusal of entry and stay.	- contribute to the prevention of illegal immigration, and - supports SIS alert on refusal of entry and stay.			- contribute to a high level of security, and - contribute to the protection of public health.		contribute to the prevention, detection and investigation of terrorist offences or of other serious criminal offences	supports SIS alerts wanted for arrest for surrender purposes or extradition purposes and alerts on persons sought to assist with a judicial procedure, for discreet checks or		

System	Main policy area	Ancillary Purposes									
									specific checks		
VIS	Article 77(2)(a)	<ul style="list-style-type: none"> - to facilitate checks at external border crossing points and within the territory of the Member States, and - supports SIS alert on refusal of entry. 	assist in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States	facilitate the application of Dublin system	<ul style="list-style-type: none"> - facilitate the visa application procedure, and - prevent the bypassing of the criteria for the determination of the Member State responsible for examining the application 	<ul style="list-style-type: none"> - to facilitate the fight against fraud, and 		<ul style="list-style-type: none"> - contribute to the prevention, detection and investigation of terrorist offences or other serious criminal offences, and - contribute to the prevention of threats to the internal security of any of the Member States; - persons wanted for arrest or for surrender or extradition purposes, missing persons or vulnerable persons, 			contribute to the correct identification of persons.

System	Main policy area	Ancillary Purposes									
								<p>persons sought to assist with a judicial procedure and persons for discreet checks, inquiry checks or specific checks;</p> <p>- support a high level of security in all Member States by contributing to the assessment of whether the applicant for or holder of a long-stay visa or a residence permit is considered to pose a threat to public policy, internal security or</p>			

System	Main policy area	Ancillary Purposes									
								public health, and - assist in the identification of persons who have gone missing, were abducted or were identified as victims of trafficking in human beings.			
EES	Article 77(2)(b) and (d) and Article 87(2)(a)	- enhance the efficiency of border checks; - enable automation of border checks on third-country nationals; - inform third-country nationals of	- assist in the identification of third-country nationals who do not or no longer fulfil the conditions for entry to, or for short stay on, the territory of the Member States;		enable visa authorities to have access to information on the lawful use of previous visas.	- gather statistics on the entries and exits, refusals of entry and overstays of third-country nationals in order to improve the assessment of the risk of overstays and support evidence-based Union migration		- contribute to the prevention, detection and investigation of terrorist offences or of other serious criminal offences, and - enable the generation of information			

System	Main policy area	Ancillary Purposes									
		<p>the duration of their authorised stay, and support</p> <p>- support national competent authorities to have access to information for the facilitation programme</p>	<p>- allow the identification and detection of overstayers and enable the competent national authorities of the Member States to take appropriate measures, and</p> <p>- allow refusals of entry in the EES to be checked electronically.</p>			<p>policy making, and</p> <p>- combat identity fraud and the misuse of travel documents.</p>		<p>for investigations related to terrorist offences or other serious criminal offences, including the identification of perpetrators, suspects and victims of those offences who have crossed the external borders.</p>			
Eurodac	Articles 78 (2)(e), 87(2)(a) and 88(2)(a) according to Regulation (EU) 603/2013			- Establish the Member State responsible for examining an application for international protection				Member States' designated authorities and Europol request the comparison of fingerprint data for law enforcement purposes.			assist in the correct identification of persons registered in Eurodac under the conditions and for the objectives referred to

System	Main policy area	Ancillary Purposes									
				lodged in a Member State by a third-country national or a stateless person, and otherwise facilitate the application of the Regulation on Asylum and Migration Management under the conditions set out in this Regulation.							in Article 20 of Regulation (EU) 2019/818 by storing identity data, travel document data and biometric data in the CIR established by that Regulation.
	Articles 78(2)(d), 78(2)(e), 78(2)(g), 79(2)(c), 87(2)(a), and 88(2)(a), according to the Eurodac Amended Proposal		- assist with the control of illegal irregular immigration to the Union and with the detection of secondary movements within the Union and with the identification	Establish the Member State responsible for examining an application for international protection lodged in a Member	- support the objectives of the VIS.	- support the objectives of ETIAS.		Member States' designated authorities and Europol may request the comparison of fingerprint and facial image biometric or alphanumeric			

System	Main policy area	Ancillary Purposes									
			n of illegally staying third-country nationals and stateless persons for determining the appropriate measures to be taken by Member States including removal and repatriation of persons residing without authorisation.	State by a third-country national or a stateless person. - assist with the application of the proposed Resettlement Regulation.				c data for law enforcement purposes for the prevention, detection or investigation of terrorist offences or of other serious criminal offences.			
SIS	Borders Article 77(2)(b) and (d), and Article 79(2)(c) of Regulation (EU) 2018/1861. Article 79(2)(c) of Regulation	Border control.	- Third-country nationals subject to return decisions issued by the Member States in the SIS; - examining the conditions and taking	- security checks on third-country nationals who apply for international protection.	- examining visa applications and taking decisions related to those applications.	- the EBCG Agency' teams for the performance of their task and as required by the operational plan for a specific operation.	Ensure the application of the provisions of Chapter 2 of Title V of Part Three TFEU relating to the movement of persons on their territories, using	- Police and customs checks; - the prevention, detection, investigation or prosecution of terrorist offences or other serious criminal offences or	- Eurojust and their assistants shall, where necessary to fulfil their mandate.	Ensure a high level of security within the area of freedom, security and justice of the Union including the maintenance of public security	

System	Main policy area	Ancillary Purposes									
	<p>(EU) 2018/1860.</p> <p>Article 82(1), Article 85(1), Article 87(2)(a) and Article 88(2)(a) of Regulation 2018/1862.</p>		<p>decisions related to the entry and stay of third-country nationals on the territory of the Member States, and to the return of third-country nationals, as well as carrying out checks on third-country nationals who are illegally entering or staying on the territory of the Member States, and</p> <p>- the EBCG Agency for the EBCG Agency' teams for return-related tasks.</p>				<p>information communicated through this system.</p>	<p>the execution of criminal penalties, and</p> <p>- Europol for the purpose of its mandate.</p>		<p>and public policy and the safeguarding of security in the territories of the Member States.</p>	

System	Main policy area	Ancillary Purposes									
ECRIS-TCN	Article 82(1), second subparagraph, point (d)								purpose of identifying the Member States where the convictions of a third country nationals were handed down		

Table 4: National authorities and Union bodies' staff with access to large-scale IT systems and interoperability components - Source: Own elaboration

Authorities/Union staff	Large-scale IT systems								
	SIS			Eurodac	VIS	EES	ETIAS	ECRIS-TCN	CIR
	Regulation (EU) 2018/1860	Regulation (EU) 2018/1861	Regulation (EU) 2018/1862	Eurodac amended proposal	VIS revised Regulation	EES Regulation	ETIAS Regulation	ECRIS-TCN Regulation	Regulations (EU) 2019/817 and 2019/818
Asylum authorities	YES Article 17(1)	YES Article 34(1)(e)	YES Article 44(1)(e)		YES Articles 21, 22, 22j, and 22k				
Border guard authorities	YES Article 17(1)	YES Article 34(1)(a)	YES Article 44(1)(a)		YES Articles 18, 21, 22(i), and 22g	YES Article 9(2)	YES Article 13(2)		YES Article 21
Carriers							YES Article 13(3)		
Central authorities of the convicting Member State								YES Articles 5 and 9	YES Article 21

Authorities/Union staff	Large-scale IT systems								
	SIS			Eurodac	VIS	EES	ETIAS	ECRIS-TCN	CIR
	Regulation (EU) 2018/1860	Regulation (EU) 2018/1861	Regulation (EU) 2018/1862	Eurodac amended proposal	VIS revised Regulation	EES Regulation	ETIAS Regulation	ECRIS-TCN Regulation	Regulations (EU) 2019/817 and 2019/818
Designated authorities	YES Article 17(1)	YES Article 34(1)(c)	YES Article 44(1)(c)	YES Article 5	YES ¹ Articles 6(3), second paragraph, 22l, and 22n	YES Article 9(3)	YES Article 50		YES Article 22
EBCG Agency	YES ² Article 17(3)	YES ³ Article 36	YES ⁴ Article 50		YES Articles 45e and 45f	YES ⁵ Article 63(1) <i>in fine</i>			
EPPO								YES Article 14	
ETIAS Central Unit	YES Article 36b of the ETIAS	YES Article 36b of the ETIAS	YES Article 36b of the ETIAS	YES Article 8a	YES Article 18c of the ETIAS	YES Article 25a of the ETIAS	YES Article 13(1)	YES Article 7b of the ETIAS	YES Article 21

¹ Limited to teams of staff involved in return-related operations.

² Access is restricted to the staff involved in return-related tasks, and members of the migration management support teams.

³ *Ibidem.*

⁴ *Ibidem.*

⁵ Access is restricted to the purposes of carrying out risk analyses and vulnerability assessments.

Authorities/Union staff	Large-scale IT systems								
	SIS			Eurodac	VIS	EES	ETIAS	ECRIS-TCN	CIR
	Regulation (EU) 2018/1860	Regulation (EU) 2018/1861	Regulation (EU) 2018/1862	Eurodac amended proposal	VIS revised Regulation	EES Regulation	ETIAS Regulation	ECRIS-TCN Regulation	Regulations (EU) 2019/817 and 2019/818
	consequential amendments	consequential amendments	consequential amendments		consequential amendments	consequential amendments		consequential amendments	
ETIAS National Unit	YES Article 25a(1)(e) of the ETIAS consequential amendments	YES Article 25a(1)(c) of the ETIAS consequential amendments	YES Article 25a(1)(d) of the ETIAS consequential amendments	YES Article 8b	YES Article 18d of the ETIAS consequential amendments	YES Article 25b of the ETIAS consequential amendments	YES Article 13(1)	YES Article 7b(1)(b) of the ETIAS consequential amendments	YES Article 21
Europol	YES Article 17(2)	YES Article 35	YES Article 48	YES Article 7	YES Article 22m	YES Article 30	YES Article 53	YES Article 14	YES Article 22
Eurojust			YES Article 49					YES Article 14	
Immigration authorities⁶, authorities competent for carrying out checks within the	YES Article 17(1)	YES Article 34(1)(d)	YES Article 44(1)(d)	YES Article 14(1)	YES Article 6(2b) and (2c), and	YES Article 9(2)	YES Article 13(4)		YES Article 21

⁶ According to the EES and the ETIAS Regulations.

Authorities/Union staff	Large-scale IT systems								
	SIS			Eurodac	VIS	EES	ETIAS	ECRIS-TCN	CIR
	Regulation (EU) 2018/1860	Regulation (EU) 2018/1861	Regulation (EU) 2018/1862	Eurodac amended proposal	VIS revised Regulation	EES Regulation	ETIAS Regulation	ECRIS-TCN Regulation	Regulations (EU) 2019/817 and 2019/818
territory of the Member States ⁷ , or authorities in charge of examining the conditions and taking decisions related to the entry and stay of third-country nationals on the territory of the Member States ⁸					Articles 22(h) and 22(i)				
Authorities competent for naturalisation	YES Article 17(1)	YES Article 34(2)							
National Access Point				YES Article 6					




⁷ According to the VIS revised Regulation.

































⁸ According to the SIS Regulations.

Authorities/Union staff	Large-scale IT systems								
	SIS			Eurodac	VIS	EES	ETIAS	ECRIS-TCN	CIR
	Regulation (EU) 2018/1860	Regulation (EU) 2018/1861	Regulation (EU) 2018/1862	Eurodac amended proposal	VIS revised Regulation	EES Regulation	ETIAS Regulation	ECRIS-TCN Regulation	Regulations (EU) 2019/817 and 2019/818
National Judicial Authorities	YES Article 17(1)	YES Article 34(3)	YES Article 44(3)						
Police and customs checks	YES Article 17(1)	YES Article 34(1)(b)	YES Article 44(1)(b)						YES Article 20
SIRENE Bureau									YES Article 21
Visa Authorities	YES Article 17(1)	YES Article 34(1)(f)	YES Article 44(1)(d)	YES Article 8c	YES Article 6(1)	YES Article 9(2)	YES Article 13(4b) of the revised VIS Regulation	YES ⁹ Article 7a2 of the VIS revised Regulation	YES Article 21

⁹ Access is restricted to those data that are flagged for terrorists or serious criminals.

Table 5: Variable geometry, large-scale IT systems and of interoperability – Source: Own elaboration

	Accessed Member States that do not fully apply the Schengen <i>acquis</i>								 This state has access to the system to enter and amend an individual file
	Schengen Associated Countries								 This state has no access to the system and cannot enter or amend an individual file
	Member States with an opt-in/opt-out regime								 This state has access to the system but has no right to enter or amend an individual file
	Member States that may implement Schengen <i>acquis</i> measures in national law								

	Systems that constitute development of the Schengen <i>acquis</i>			Hybrid			Systems that do not constitute development of the Schengen <i>acquis</i>	
	EES	VIS	ETIAS ¹⁰	SIS			ECRIS-TCN	Eurodac
				2018/1861	2018/1860	2018/1862		
Austria								
Belgium								
Bulgaria	 ¹¹	 ¹²						
Croatia	 ¹³	 ¹⁴		 ¹⁵				

¹⁰ ETIAS' individual files are created as soon as the ETIAS form is submitted by the applicant, which does not require the intervention of national authorities. The identity files stored in ETIAS can be modified only upon request of the visa exempt third country nationals according to Article 64 of the ETIAS Regulation.

¹¹ Bulgaria will implement the EES since the verification in accordance with the applicable Schengen evaluation procedure has already been successfully completed and the provisions of the Schengen *acquis* relating to the SIS, established by Regulation (EC) No 1987/2006, have been put into effect in accordance with the relevant Act of Accession – see Article 4(2) of the Protocol concerning the conditions and arrangements for admission of the Republic of Bulgaria and Romania to the European Union, *OJ L* 157, 21.6.2005, pp. 29-202. Specific conditions of the EES Regulation regarding the operation of the EES apply for land-borders – see Article 4(4) and (5) of the EES Regulation.

¹² Although tests have been successfully completed, Bulgaria has to notify it to the European Commission so that the latter can issue a decision on the starting date. Bulgaria has been granted passive access to the VIS for the purpose of operating the EES which allows Bulgaria to consult VIS data without the right to insert or modify identity files. See the Council Decision (EU) 2017/1908 of 12 October 2017 on the putting into effect of certain provisions of the Schengen *acquis* relating to the Visa Information System in the Republic of Bulgaria and Romania, *OJ L* 269, 19.10.2017, pp. 39-43. However, passive access to the VIS does not apply to long-stay permissions foreseen by the revised VIS Regulation. Full use of the system will be granted through a Council decision formally admitting Bulgaria to the Schengen area.

¹³ Croatia will not use the EES until it accomplishes with the SCH-EVAL.

¹⁴ Croatia will not use the VIS until it accomplishes with the SCH-EVAL and a Council decision formally admits Croatia to the Schengen area.

¹⁵ Croatia will not use the SIS alerts for refusal of entries until it will accomplish with the SCH-EVAL.

	Systems that constitute development of the Schengen <i>acquis</i>			Hybrid			Systems that do not constitute development of the Schengen <i>acquis</i>	
	EES	VIS	ETIAS ¹⁰	SIS			ECRIS-TCN	Eurodac
				2018/1861	2018/1860	2018/1862		
Cyprus	⊘ ¹⁶	⊘ ¹⁷	🚫	⊘ ¹⁸	⊘ ¹⁹	⊘ ²⁰	🚫	🚫
Czechia	🚫	🚫	🚫	🚫	🚫	🚫	🚫	🚫
Denmark	🚫	🚫 ²¹	🚫	🚫	🚫	🚫	⊘ ²²	🚫 ²³
Estonia	🚫	🚫	🚫	🚫	🚫	🚫	🚫	🚫
Finland	🚫	🚫	🚫	🚫	🚫	🚫	🚫	🚫
France	🚫	🚫	🚫	🚫	🚫	🚫	🚫	🚫
Germany	🚫	🚫	🚫	🚫	🚫	🚫	🚫	🚫
Greece	🚫	🚫	🚫	🚫	🚫	🚫	🚫	🚫
Hungary	🚫	🚫	🚫	🚫	🚫	🚫	🚫	🚫
Iceland	🚫	🚫	🚫	🚫	🚫	👁️ ²⁴	⊘	🚫 ²⁵

¹⁶ Cyprus will not use the EES until it accomplishes the SCH-EVAL.

¹⁷ Cyprus will not use the VIS until it accomplishes the SCH-EVAL and a Council decision formally admits Cyprus to the Schengen area.

¹⁸ Cyprus will not use the SIS alerts until it accomplishes the SCH-EVAL.

¹⁹ *Ibidem*.

²⁰ *Ibidem*.

²¹ Should Denmark want to apply the revised VIS, it has to notify its willingness to participate in the revised VIS Regulation.

²² For the time being, Denmark has not concluded an agreement with the EU to participate in the ECRIS-TCN.

²³ Agreement between the European Community and the Kingdom of Denmark on the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in Denmark or any other Member State of the European Union and “Eurodac” for the comparison of fingerprints for the effective application of the Dublin Convention, *OJ L 66*, 8.3.2006, p. 37.

²⁴ Except for the alerts on Arrest Warrant since Iceland does not take part to the enhanced cooperation. However, the alerts of the other Member States are visible.

²⁵ Agreement between the European Community and the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Iceland or Norway, *OJ L 93*, 3.4.2001, p. 40.

	Systems that constitute development of the Schengen <i>acquis</i>			Hybrid			Systems that do not constitute development of the Schengen <i>acquis</i>	
	EES	VIS	ETIAS ¹⁰	SIS			ECRIS-TCN	Eurodac
				2018/1861	2018/1860	2018/1862		
Ireland ²⁶	⊘	⊘	⊘	⊘	⊘	🔍 ²⁷	⊘ ²⁸	🔍 ²⁹
Italy	🔍	🔍	🔍	🔍	🔍	🔍	🔍	🔍
Latvia	🔍	🔍	🔍	🔍	🔍	🔍	🔍	🔍
Liechtenstein	🔍	🔍	🔍	🔍	🔍	🔍	⊘	🔍 ³⁰
Lithuania	🔍	🔍	🔍	🔍	🔍	🔍	🔍	🔍
Luxembourg	🔍	🔍	🔍	🔍	🔍	🔍	🔍	🔍
Malta	🔍	🔍	🔍	🔍	🔍	🔍	🔍	🔍
Netherlands	🔍	🔍	🔍	🔍	🔍	🔍	🔍	🔍
Norway	🔍	🔍	🔍	🔍	🔍	👁️ ³¹	⊘	🔍 ³²
Poland	🔍	🔍	🔍	🔍	🔍	🔍	🔍	🔍
Portugal	🔍	🔍	🔍	🔍	🔍	🔍	🔍	🔍

²⁶ Should Ireland want to implement the systems that constitute a development of the Schengen *acquis*, then, an amendment to the Council Decision 2004/926/EC, of 22 December 2004 on the putting into effect of parts of the Schengen *acquis* by the United Kingdom of Great Britain and Northern Ireland, *OJ L* 395, 31.12.2004, pp. 70-80, would be needed. In this way, Ireland would also adhere to the correspondent EU competences on borders and migration.

²⁷ See the Council implementing decision (EU) 2020/1745 of 18 November 2020 on the putting into effect of the provisions of the Schengen *acquis* on data protection and on the provisional putting into effect of certain provisions of the Schengen *acquis* in Ireland, *OJ L* 193/3, 23.11.2020, pp. 3-11.

















































²⁸ From the time being, Ireland has not opted-in into ECRIS-TCN but it potentially notifies its willingness in the future.

²⁹ Ireland opted-in Eurodac according to the Commission Decision on the Request by Ireland to accept Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast) , 11 December 2014, C(2014)9310 final.

³⁰ Protocol between the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland, *OJ L* 160 18.6.2011 p. 39.

³¹ Except for the alerts on Arrest Warrant since Norway does not take part to enhanced cooperation. However, the alerts of the other Member States are visible to Norway.

³² Agreement between the European Community and the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Iceland or Norway, *OJ L* 93, 3.4.2001, p. 40.

	Systems that constitute development of the Schengen <i>acquis</i>			Hybrid			Systems that do not constitute development of the Schengen <i>acquis</i>	
	EES	VIS	ETIAS ¹⁰	SIS			ECRIS-TCN	Eurodac
				2018/1861	2018/1860	2018/1862		
Romania	 ³³	 ³⁴						
Slovakia								
Slovenia								
Spain								
Sweden								
Switzerland								 ³⁵

³³ Romania will operate the EES since the verification in accordance with the applicable SCH-EVAL has already been successfully completed, the passive access to the VIS established by Council Decision 2004/512/EC has been granted for the purpose of operating the EES, and the provisions of the Schengen *acquis* relating to the SIS, established by Regulation (EC) No 1987/2006, have been put into effect in accordance with the relevant Act of Accession – see Article 4(2) of the Protocol concerning the conditions and arrangements for admission of the Republic of Bulgaria and Romania to the European Union, *OJ L* 157, 21.6.2005, pp. 29-202. Specific conditions of the EES Regulation for the operation of EES apply for land-borders – see Article 4(4) and (5) of the EES Regulation.

³⁴ Romania has been granted passive access to the VIS that allows it to consult VIS data without the right to enter or modify identity files according to the Council Decision (EU) 2017/1908 of 12 October 2017 on the putting into effect of certain provisions of the Schengen *acquis* relating to the Visa Information System in the Republic of Bulgaria and Romania, *OJ L* 269, 19.10.2017, pp. 39-43. However, passive access to the VIS does not apply to long-stay permissions of the revised VIS Regulation. Full use of the system will be granted once a Council decision formally admits Croatia into the Schengen area.

³⁵ Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland, *OJ L* 53, 27.2.2008, p. 5.

Table 6: Data stored in the Common Identity Repository - Source: Own elaboration

Interoperability component	IO Regulations	Large-scale IT systems		Fingerprints or dactyloscopic data	Facial image	Alphanumeric data	Travel document
CIR ³⁶	Article 18 Regulation (EU) 2019/817	EES Regulation	VISA third-country nationals	Article 18(2)(c) when they are refused to enter, there is no previous file with biometric in the EES and they are not registered in the VIS	Article 16(1)(d) And Article 18(2)(a) when they are refused to enter and there is no previous file with biometric in the EES or (c) if they are not registered in the VIS	Article 16(1)(a) refers to: surname (family name); first name or names (given names); date of birth; nationality or nationalities, and sex And Article 18(1)(a) if they are refused to enter and where no previous file is recorded in the EES, recalling Article 16(1)(a)	Article 16(1)(b) refers to: the type and number of the travel document or documents and the three letter code of the issuing country of the travel document or documents And Article 16(1)(c) refers to: the date of expiry of the validity of the travel document or documents And Article 18(1)(a) if they are refused to enter and where no previous file is recorded in the EES, recalling Article 16(1)(b)(c)
			VISA exempt third-country nationals	Article 17(1)(c) And Article 18(2)(b) when they are refused to enter and there is no previous file with biometric in the EES	Article 17(1)(b) And Article 18(2)(b) when they are refused to enter and there is no previous file with biometric in the EES	Article 17(1)(a) recalling Article 16(a): surname (family name); first name or names (given names); date of birth; nationality or nationalities, and sex And Article 18(1)(b) recalling Article 17(1) if they are refused to enter and there is no previous file with biometric in the EES	Article 17(1)(a) recalling Article 16 (b) and (c): the type and number of the travel document or documents and the three letter code of the issuing country of the travel document or documents; the date of expiry of the validity of

³⁶ The Schengen Information System (SIS II) is out of the CIR.

							the travel document or documents And Article 18(1)(b) recalling Article 17(1) if they are refused to entry and where no previous file is recorded in the EES
		VIS revised Regulation		Articles 5(b) And Article 22a(k)	Article 5(c) ³⁷ And Article 22a(j)	Article 5 letter (a): surname (family name); first name or names (given names); date of birth, sex And letter (aa): surname at birth (former surname(s)); place and country of birth; current nationality and nationality at birth And Article 22a(d): surname (family name), first name(s), date of birth, current nationality or nationalities, sex, place of birth	Article 9(4)(b): the type and number of the travel document or documents and the three-letter code of the issuing country of the travel document or documents And (c): the date of expiry of the validity of the travel document or documents ³⁸ And Article 22a(e) to (g): type and number of the travel document; the date of expiry of the validity of the travel document; the country which issued the travel document and its date of issue
		ETIAS Regulation				Article 17(2)(a): surname (family name), first name(s) (given name(s)), surname at birth; date of birth, place of birth, sex, current nationality, And	Article 17(2)(d): type, number and country of issue of the travel document And

³⁷ The VIS Regulation 767/2008 includes photographs under Article 9(5) and these are stored in the CIR according to Article 5(1a) of the VIS revised Regulation. Photographs are included in the CIR according to Article 18(1)(b) of Regulation (EU) 2019/817.

³⁸ Article 5(1a) of the VIS revised Regulation refers to Article 9(4)(ca) of the VIS Regulation, but the data on ‘the authority which issued the travel document and its date of issue’ should not be stored in the CIR according to Article 4(13) of Regulation (EU) 2019/817.

					(aa): country of birth, first name(s) of the parents of the applicant ³⁹ And (b): other names (alias(es), artistic name(s), usual name(s)), if any And (c): other nationalities, if any	(e): the date of issues ⁴⁰ and the date of expiry of the validity of the travel document
	Article 18 Regulation (EU) 2019/818	ECRIS-TCN Regulation	Article 5(1)(b) (i) and (ii)	Article 5(3) ⁴¹	Regulation 818/2019 lists those data of Article 5(1) that are stored in the CIR: (a)(i) stands for surname (family name), first name (given names), date of birth, place of birth (town and country), nationality or nationalities, gender, previous names, if applicable, And (iii), second part stands for: pseudonyms or aliases	Regulation 818/2019 refers to 'information on travel documents' according to its definition set for in Article 4(14). According to Article 5(1)(a)(iii), first part, the CIR includes: identity number, or the type and number of the person's identification documents

³⁹ Article 18(1)(c) of the IO Regulations refers to Article 17(2)(a) to (e) of the ETIAS Regulation, but letter (aa) of Article 17 of the ETIAS Regulation includes both country of birth and first name(s) of the parents of the applicant. The latter should be excluded.

⁴⁰ Article 17(2)(e) of the ETIAS Regulation refers both to the date of issue and the date of expiry of the validity of the travel document but the CIR should store only the latter. The date of issues should stay out of the CIR.

⁴¹ Regulation (EU) 2019/818 refers to Article 5(2) of the ECRIS-TCN Regulation, but this Article watch over data quality. Article 5(3) refers to facial recognition instead.

Table 7: Data stored in the shared Biometric Matching Service - Source: Own elaboration

Interoperability component	IO Regulations	Large-scale IT systems		Fingerprints or dactyloscopic data	Facial image	Alphanumeric data	Travel document
sBMS ⁴²	Article 13 Regulation (EU) 2019/817 ⁴³	EES Regulation	VISA third-country nationals	Article 18(2)(c) when they are refused to enter, there is no previous file with biometric data in the EES and they are not already registered in the VIS	Article 16(1)(d) And Article 18(2)(a) when they are refused to enter and there is no previous file with biometric data in the EES or (c) if they are not already registered in the VIS		
			VISA exempt third-country nationals	Article 17(1)(c) And Article 18(2)(b) when they are refused to enter and there is no previous file with biometric data in the EES	Article 17(1)(b) And Article 18(2)(b) when refused to enter and there is no previous file with biometric data in the EES		
		VIS revised Regulation		Articles 5(b) And Article 22a(k)	Article 5(c) And Article 22a(j)		
		SIS Regulation (EU) 2018/1861		Article 20(2)(x)	Article 20(2)(w) ⁴⁴		
		SIS Regulation (EU) 2018/1860		Article 4(1)(v) ⁴⁵	Article 4(1)(u) ⁴⁶		
		SIS Regulation (EU) 2018/1862		Article 20(3)(y)	Article 20(3)(w) ⁴⁷		

⁴² The sBMS does not include ETIAS because does not ETIAS store biometrics.

⁴³ The sBMS does not store palm prints.

⁴⁴ Regulation 2018/1861 sets forth that the SIS also stores photographs according to Article 4(11) of the IO Regulations.

⁴⁵ Article 4(3) of Regulation 2018/1860 allows for the processing of palm prints, but palm prints are excluded from the sBMS.

⁴⁶ Regulation 2018/1860 provides for the storage of photographs too.

⁴⁷ Regulation 2018/1862 stores photographs too.

	Article 13 Regulation (EU) 2019/818	ECRIS-TCN Regulation	Article 5(1)(b) (i) and (ii)	Article 5(3) ⁴⁸		
--	---	----------------------	-------------------------------------	----------------------------	--	--

⁴⁸ Regulation (EU) 2019/818 refers to Article 5(2) of the ECRIS-TCN Regulation, but this Article watch over data quality. Article 5(3) refers to facial recognition instead.

Table 8: Data stored in the Multiple Identity Detector - Source: Own elaboration

Interoperability component	IO Regulations	Large-scale IT systems		Fingerprints or dactyloscopic data	Facial image	Alphanumeric data	Travel document
MID ⁴⁹	Article 27 Regulation (EU) 2019/817	EES Regulation	VISA TCN	<p>Article 18(2)(c)</p> <p>when they are refused to enter, there is no previous file with biometric data in the EES and they are not already registered in the VIS</p>	<p>Article 16(1)(d)</p> <p>And</p> <p>Article 18(2)(a) when they are refused to enter and there is no previous file with biometric data in the EES or (c) if they are not already registered in the VIS</p>	<p>Article 16(1)(a) refers to: surname (family name); first name or names (given names); date of birth; nationality or nationalities; sex</p> <p>And</p> <p>Article 18(1)(a) if they are refused to enter, recalling Article 16(1)(a)</p>	<p>Article 16(1)(b) refers to: the type and number of the travel document or documents and the three letter code of the issuing country of the travel document or documents</p> <p>And</p> <p>Article 16(1)(c): the date of expiry of the validity of the travel document or documents</p> <p>And</p> <p>Article 18(1)(a) recalling Article 16(1)(b)(c) if they are refused to enter and where no previous file is recorded in the EES</p>
			VISA exempt third-country nationals	<p>Article 17(1)(c)</p> <p>And</p> <p>Article 18(2)(b) when they are refused to enter and there is no previous file with biometric data in the EES</p>	<p>Article 17(1)(b)</p> <p>And</p> <p>Article 18(2)(b) when refused to enter and there is no previous file with biometric data in the EES</p>	<p>Article 17(1)(a) recalls Article 16(a): surname (family name); first name or names (given names); date of birth; nationality or nationalities; sex</p> <p>And</p> <p>Article 18(1)(b) which recalls Article 17(1) when they are refused to enter</p>	<p>Article 17(1)(a) which recalls Article 16(1)(b): the type and number of the travel document or documents and the three letter code of the issuing country of the travel document or documents</p> <p>And also recalls</p> <p>(c): the date of expiry of the validity of the travel document or documents</p>

⁴⁹ The Multiple Identity Detector (MID) is not a database and the data listed are only used for comparison. The MID receives orders from the European Search Portal (ESP) to compare data retained by the CIR and the SIS. In order to execute the orders, the CIR and the SIS use the sBMS for biometric data and the ESP for alphanumeric data.

							And Article 18(1)(b) recalling Article 17(1) if they are refused to enter and where no previous file is recorded in the EES
		VIS revised Regulation				<p>Article 5 letter (a): surname (family name); first name or names (given names); date of birth, sex</p> <p>And</p> <p>letter (aa): surname at birth (former surname(s)); place and country of birth; current nationality and nationality at birth</p> <p>And</p> <p>Article 22a(d): surname (family name), first name(s), date of birth, current nationality or nationalities, sex, place of birth</p>	<p>Article 9(4)(b): the type and number of the travel document or documents and the three-letter code of the issuing country of the travel document or documents</p> <p>And</p> <p>(c): the date of expiry of the validity of the travel document or documents⁵⁰</p> <p>And</p> <p>Article 22a(e) to (g): type and number of the travel document; the date of expiry of the validity of the travel document; the country which issued the travel document and its date of issue</p>
		ETIAS Regulation				<p>Article 17(2)(a): surname (family name), first name(s) (given name(s)), surname at birth; date of birth; place of birth: country of birth: sex, current nationality</p> <p>And</p> <p>(b): other names (alias(es), artistic name(s), usual name(s))</p> <p>And</p>	<p>Article 17(2)(d): type, number and country of issues of the travel document</p> <p>And</p> <p>(e): the date of expiry of the validity of the travel document</p>

⁵⁰ Article 5(1a) of the VIS revised Regulation refers to Article 9(4)(ca) of the VIS Regulation, but the data on ‘the authority which issued the travel document and its date of issue’ should not be stored in the CIR according to Article 4(13) of Regulation (EU) 2019/817.

					(c): other nationalities, if any	
		SIS Regulation (EU) 2018/1861	Article 20(2)(x)	Article 20(2)(w)	Article 20(2)(a)(b)(c)(d)(f)(g)(h)(i): surnames; forenames; names at birth; previously used names and alias; place of birth; date of birth; gender and any nationalities held	Article 20(2)(s)(t)(u)(v): the country of issue of the person's identification number; the number(s) of the person's identification documents
		SIS Regulation (EU) 2018/1860	Article 4(1)(v)	Article 4(1)(u)	Article 4(1)(a) to (h): surnames; forenames; names at birth; previously used names and aliases; place of birth; date of birth; gender and any nationalities held	Article 4(1)(q) to (s): the category of the person's identification documents; the country of issue of the person's identification documents; the number(s) of the person's identification documents
	Article 27 Regulation (EU) 2019/818	SIS Regulation (EU) 2018/1862	Article 20(3)(y)	Article 20(3)(w)	Article 20(3)(a) to (d): surnames; forenames; names at birth; previously used names and aliases And (f) to (i): place of birth; date of birth; gender; any nationalities held	Article 20(3)(s) to (u): the category of the person's identification documents; the country of issue of the persons' identification documents; the number(s) of the person's identification documents
		ECRIS-TCN Regulation	Article 5(1)(b) (i) (ii)	Article 5(3) ⁵¹	Article 5(1)(a)(i): surname (family name); first names (given names); date of birth; place of birth (town and country); nationality or nationalities; gender; previous names, if applicable And (iii), second part: pseudonyms or aliases ⁵²	Article 5(1)(a)(iii), first part: identity number; or the type and number of the person's identification documents

⁵¹ Regulation (EU) 2019/818 refers to Article 5(2) of the ECRIS-TCN Regulation, but this watches over data quality. Article 5(3) refers to facial recognition.

⁵² Previous names, if applicable, and pseudonyms or aliases are not listed in Article 27(3)(b) of Regulation (EU) 2019/818, but they are stored in the CIR. The ECRIS-TCN Regulation mentions them too, so the MID should process them.