Revista Española de Derecho Europeo
Núm. 76 | Octubre – Diciembre 2020
pp. 111-162
Madrid, 2020
DOI:10.37417/num_76_2020_532

ISSN: 2695-7191
Recibido: 10/11/2020 | Aceptado: 16/12/2020

LA SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA EN EL ASUNTO *SCHREMS II* O COMO LOS DATOS PERSONALES PUEDEN TERMINAR VIAJANDO SIN EQUIPAJE

THE JUDGMENT OF THE COURT OF JUSTICE OF THE EUROPEAN UNION IN THE *SCHREMS II* CASE, OR HOW PERSONAL DATA CAN END UP TRAVELING WITHOUT BAGGAGE

Susana Ruiz Tarrías*

RESUMEN: El grado de interconexión de las sociedades actuales conlleva la necesidad de realizar transferencias internacionales de datos personales que, en todo caso, deben garantizar la protección de los derechos a la vida privada y a la protección de datos personales de los ciudadanos europeos (arts. 7 y 8 CDFUE). La Unión Europea ha articulado desde 1999 dos marcos normativos para las transferencias de datos personales UE-EE.UU, el sistema de Puerto Seguro (Safe Harbor) y el Escudo de Privacidad (Privacy Shield). En ambos casos, el Tribunal de Justicia de la Unión Europea ha declarado la invalidez de la decisión de adecuación que proporcionaba soporte jurídico en el ordenamiento de la Unión a las transferencias de datos personales a uno y otro lado del Atlántico.

Sin embargo, tras la aplicación efectiva del RGPD en todos los Estados miembros, la Sentencia del Tribunal de Justicia de 16 de julio 2020 en el asunto Schrems II, parece extender en abstracto el nivel de garantía sustancialmente equivalente con el proporcionado por el ordenamiento de la Unión Europea, tanto a las transfe-

* Profesora Titular de Derecho Constitucional. Universidad de Granada Correo-e: starrias@ugr.es. ORCID: 0000-0002-8950-7072.
El presente trabajo no ha contado con ninguna financiación directa o indirecta procedente de entidad alguna, pública o privada, con o sin ánimo de lucro.

rencias internacionales basadas en decisiones de adecuación como a aquellas fundadas en cláusulas contractuales tipo. Una equiparación de las garantías a las que se une la prohibición de otorgar primacía con carácter general a las exigencias de seguridad pública, defensa o seguridad del Estado por las autoridades públicas del tercer país respecto de los datos de los ciudadanos europeos que son objeto de transferencia internacional.

PALABRAS CLAVE: UE-EEUU; transferencia datos personales; RGPD; Schrems II.

ABSTRACT: The degree of interconnection of today's societies entails the need to carry out international transfers of personal data which, in any case, must guarantee the protection of European citizens'rights to privacy and personal data protection (Articles 7 and 8 CFREU). The European Union has articulated since 1999 two regulatory frameworks for the transfer of personal data EU-US, the Safe Harbor system and the Privacy Shield. In both cases, the European Union Court of Justice has declared the invalidity of the decision of adequacy that provided legal support in the European Union system to the transfers of personal data to both sides of the Atlantic.

However**,** after the effective application of the RGPD in all Member States, the Court of Justice's Ruling of 16 July 2020 in the Schrems II case seems to extend in the abstract the level of guarantee substantially equivalent to the European Union system, both to international transfers based on adequacy decisions and those based on standard contractual clauses. An equalization of the guarantees to which is added the prohibition to grant primacy with a general character to the requirements of public security, defense or state security by the public authorities of the third country with respect to the data of European citizens who are subject of international transfer.

KEYWORDS: EU-US; personal data transfer; GDPR; Schrems II.

INTRODUCCIÓN

El pasado 20 de septiembre, cuando este trabajo todavía se encontraba en proceso de elaboración, se publicaba en *The Sunday Business Post*[1] la noticia de que la red social Facebook había comunicado al Tribunal Superior de Irlanda (*High Court*), la imposibilidad de seguir operando en la Unión Europea si se le impide transferir datos a los EEUU. Una decisión que de hacerse efectiva vendría determinada precisamente por el que constituye el objeto de estudio de este artículo, la Sentencia del Tribunal de Justicia de la Unión Europea (en adelante TJUE) de 16 de julio de 2020, en el conocido como asunto *Schrems II* acerca de las transferencias de datos personales UE-EEUU realizadas en el marco del conocido como Escudo de Privacidad o *Privacy Shield*.

Según ha declarado el TJUE en diferentes ocasiones, la comunicación de datos de carácter personal, junto a su conservación y acceso por autoridades públicas constituyen una injerencia en los derechos fundamentales consagrados en los arts. 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea (en adelante CDFUE) y del art. 8 de la Convención Europea de los Derechos Humanos (en adelante CEDH), sea cual fuere la utilización posterior de los datos comunicados y con independencia del carácter o no sensible de los datos o de que los interesados hayan sufrido o no inconvenientes derivados de la injerencia.

De hecho, según reconoció en el asunto *Parlamento/Consejo y Comisión* (2006) (par. 56) y reitera en la Sentencia de 6 de octubre de 2015 en el asunto *Schrems I* (2015) (par. 45), la operación consistente en transferir datos personales de un Estado miembro a un tercer país "constituye en sí misma un tratamiento de datos personales" en el sentido de la normativa europea.

Las páginas que siguen pretenden dar a conocer los avatares por los que han atravesado las transferencias de datos personales entre la Unión Europea y los EEUU desde 1999 en el contexto de la derogación de la Directiva 95/46/CE por el Reglamento (UE) 2016/679 (RGPD). Una nueva regulación europea en materia de protección de datos personales en virtud de la cual se lleva a cabo una reforma "de gran calado" en lo que Ortega Giménez y Gonzalo Domenech (2018) denominan la "sociedad del dato" (p. 4).

Un relato —una "historia de nudos gordianos" en palabras de Svantesson (2016, p. 39)—, en el que los aspectos jurídicos aparecen relacionados con la

[1] https://www.businesspost.ie/legal/facebook-fears-ruling-may-force-it-to-pull-social-media-platforms-from-eu-00644da4.

descripción de ciertas técnicas de intervención de los poderes públicos que bajo la cobertura de la protección de la seguridad pública, la defensa y la seguridad del Estado, llevan a cabo un tratamiento de los datos personales de los ciudadanos que circulan a nivel mundial a través de internet. Una injerencia de los poderes públicos que evidencia los riesgos a los que se exponen los derechos fundamentales de los ciudadanos cuando son objeto de transferencia a terceros países ajenos al Espacio Económico Europeo (en adelante EEE)[2].

El punto de partida en el análisis de las transferencias internacionales de datos personales se sitúa en la constatación de que las sociedades actuales interactúan en aspectos tan relevantes que se paralizarían si no fuera posible la transferencia de información entre países. Pero del mismo modo que el derecho a la protección de datos no se configura en los ordenamientos jurídicos occidentales como un derecho de carácter absoluto, el gigantesco flujo de información que genera la globalización no puede suponer, ni siquiera en garantía de la seguridad de Estados que se adjetivan como "democráticos" y "de Derecho" una limitación de las garantías adecuadas de los derechos fundamentales de los ciudadanos.

En especial, el derecho a la vida privada y a la protección de datos de carácter personal constituyen elementos conformadores del espacio de libertad individual que, todavía hoy, cabe identificar, como hiciera Constant (1819) en su conocido discurso pronunciado en el Ateneo de París, con la "libertad de los modernos" en contraposición a la "libertad de los antiguos", donde "todas las acciones privadas", incluso las domésticas, "estaban sometidas a una severa vigilancia" y eran objeto de intervención "de la autoridad" (p. 594).

El presente estudio analiza, en primer término, los elementos conceptuales y los instrumentos previstos en el actual Reglamento (UE) General de Protección de Datos (en adelante RGPD) para llevar a cabo lícitamente el tránsito de datos personales desde la UE a terceros países.

En un segundo bloque de contenidos se describe el primer marco jurídico para las transferencias de datos personales conocido como Puerto Seguro (*Safe Harbor*), articulado entre la UE y los EE.UU a partir de las previsiones contempladas en la Directiva 95/46/CE, las carencias manifestadas desde sus primeros momentos de aplicación y, en última instancia, la declaración de su invalidez por el TJUE en el asunto *Schrems I* anulando la decisión de adecuación que sustentaba la licitud de dichas transferencias de datos (Decisión 2000/520/CE).

---

[2] Como resulta conocido el RGPD es de aplicación al Espacio Económico Europeo (EEE) que incluye a los Estados miembros de la UE junto a Islandia, Liechtenstein y Noruega. Así se reconoce en la rúbrica de la norma al afirmar que se trata del "Texto pertinente a efectos del EEE". No obstante, el art. 3 RGPD se define su ámbito territorial de aplicación por referencia a la Unión, al igual que sucede con el conjunto de la regulación.

El tercer nivel de análisis viene constituido por el estudio del marco jurídico adoptado con posterioridad al Puerto Seguro para llevar a cabo las transferencias de datos UE-EEUU denominado Escudo de Privacidad (*Privacy Shield*). Articulado también bajo la vigencia de la Directiva 95/46/CE teóricamente toma en consideración las apreciaciones realizadas por el TJUE en el asunto *Schrems I* respecto de su predecesor el Puerto Seguro. Sin embargo, distintos organismos europeos como el Grupo de Trabajo de protección de las personas en lo que respecta al tratamiento de datos personales o Working Party on the Protection of Individuals with Regard to the Processing of Personal Data (en adelante WP)[3], el Comité Europeo de Protección de Datos (en adelante CEPD o EDPB por sus siglas en inglés)[4], e instituciones de la Unión como el Parlamento Europeo pusieron de manifiesto desde su adopción importantes deficiencias que afectaban a la protección de los datos transferidos en el marco del Escudo de Privacidad.

En el último de los apartados se describen los argumentos que han llevado al TJUE en el asunto *Schrems II* a declarar la invalidez de la Decisión de Ejecución 2016/1250. Desde un punto de vista cronológico se toma en consideración la reformulación de la demanda del Sr. Schrems a instancias de la autoridad irlandesa de protección de datos, la posterior decisión de la High Court (Tribunal Superior de Irlanda) de promover distintas cuestiones prejudiciales al Alto Tribunal de la UE a partir de las constataciones llevadas a cabo por sí misma en un pronunciamiento anterior, y los razonamientos en los que el Tribunal de Justicia fundamenta la validez de la Decisión de la Comisión 2010/87/UE (Decisión CPT) y la invalidez de la Decisión de Ejecución 2016/1250 (Decisión EP) en la que se fundamentaba el Escudo de Privacidad.

1. ASPECTOS GENERALES DE LAS TRANSFERENCIAS INTERNACIONALES DE DATOS EN EL MARCO DE LA UE

1.1. Aproximación al concepto de transferencia internacional de datos personales

Como punto de partida, debe tomarse en consideración que el término transferencia internacional de datos personales constituye una expresión que convive en el ámbito doctrinal junto a otras locuciones como transmisión internacional de datos, flujo internacional de datos o movimiento internacio-

[3] A lo largo del texto se utilizará el acrónimo en inglés WP en tanto que los documentos consultados no tienen versión española y aparecen citados en la bibliografía en la versión inglesa.

[4] A lo largo del texto se utilizará el doble acrónimo en español e inglés CEPD-EDPB, habida cuenta de que algunos documentos consultados no tienen versión española y aparecen citados en la bibliografía en la versión inglesa.

nal de datos, aunque tanto las normas internacionales como las regulaciones europea y nacional optan por utilizar el concepto de transferencia internacional.

Así, el término transferencia es el que viene siendo utilizado por el legislador de la Unión desde la adopción de la Directiva 95/46/CE hasta el actual RGPD aunque ninguna de las normas antes mencionadas incorpora una definición de lo que debe entenderse como transferencia de datos personales a un país tercero, como reconoció el TJUE respecto de la Directiva comunitaria en el asunto *Bodil Lindqvist* (2003, par. 56).

En todo caso, el RGPD hace posible una clarificación de este concepto a través de la contraposición entre la transferencia internacional de datos y el tratamiento transfronterizo de datos personales. Este último término es definido en el art. 4(23) RGPD con referencia a un tratamiento de datos personales realizado en el contexto territorial de Estados miembros de la UE[5].

De este modo, un elemento a tomar en consideración atendiendo a la regulación de la Unión Europea para concretar el concepto de transferencia internacional de datos personales, proviene de la circunstancia de que esta debe suponer la involucración de un tercer país u organización internacional no perteneciente a la Unión Europea en el tratamiento de datos personales con origen en la Unión.

En todo caso, la aproximación a una definición de transferencia internacional de datos personales se ha abordado por la doctrina y la jurisprudencia tomando en consideración los siguientes elementos:

a) Debe tratarse de datos de carácter personal, lo que supone que el tratamiento de datos viene referido a personas físicas identificadas o identificables no fallecidas, según el concepto de "datos personales" proporcionado por el art. 4(1) RGPD, es decir, "toda información sobre una persona física identificada o identificable" ("el interesado").

A tales efectos, se considerará persona física susceptible de identificación según dicho precepto:

> "toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios

[5] En el ámbito del Consejo de Europa, el reciente Protocolo núm. 223 por el que se modifica el Convenio de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE núm. 108), acordado durante la 128.ª sesión del Comité de Ministros en Elsinore (Dinamarca) los días 17 y 18 de mayo de 2018, conocido como Convenio 108+ (o Convenio 108 *modernizado), utiliza en su art. 14 el término "flujos transfronterizos" de datos personales. La Resolución legislativa del Parlamento Europeo de 12 de marzo de 2019 sobre la propuesta de Decisión del Consejo, ha autorizado a los Estados miembros la firma de dicho Protocolo.*

> elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

b) Los datos personales deben ser objeto de un tratamiento total o parcialmente automatizado, o bien de un tratamiento no automatizado en el que los datos personales se incluyan o estén destinados a ser incluidos en un fichero (art. 2 RGPD).

El simple tránsito de información no supone una transferencia internacional de datos personales, pues para hablar de esta última tendremos que atender al tratamiento que los datos personales reciban en el tercer país (Ustarán y García, 2019). Así lo entendió, por lo demás, el TJUE en el citado asunto *Bodil Lindqvist*.

En su opinión, no existe transferencia internacional de datos en el sentido del art. 25 de la Directiva 95/46/CE cuando

> "una persona en un Estado miembro difunde datos personales en una página web almacenada por un proveedor que tiene su domicilio en el mismo Estado o en otro Estado miembro de la Unión, de modo que dichos datos resultan accesibles a cualquier persona que se conecte a Internet, incluidas aquéllas que se encuentren en países terceros" (par. 71).

En consecuencia, no estaríamos ante una transferencia internacional cuando una persona hace públicos —difunde— datos personales en una página web almacenada en un servidor de la UE aunque resulten accesibles a nacionales de terceros Estados. Para que exista transferencia internacional de datos el TJUE exige, en un pronunciamiento "arriesgado" según Poullet (2007, p. 97), que los datos personales hayan sido objeto de "una transferencia directa" entre quien publica los datos en una página web y quien los recibe en su ordenador en un tercer país (asunto *Bodil Lindqvist*, par. 61).

Atendiendo a las consideraciones expresadas por el TJUE en el asunto *Bodil Lindqvist* la transferencia internacional de datos personales implica el envío de datos de un Estado miembro a un tercer país u organización internacional donde dichos datos son objeto de tratamiento[6]. No obstante, cons-

---

[6] A partir de esta premisa, Ustarán y García (2019) estiman que existen diferentes criterios doctrinales acerca, por ejemplo, de la aplicación del concepto de transferencia internacional de datos respecto de internet, el correo electrónico y las páginas web que pueden suponer "transferencias aleatorias" de datos personales entre "servidores intermedios" a pesar de que los servidores de origen y destino se encuentren en el mismo país (p. 462).

Más clara resulta la procedencia de hablar de transferencia internacional de datos en referencia a la prestación de servicios de computación en la nube o *cloud computing* si estamos ante un tratamiento de datos desarrollado a partir del envío de la información a terceros países (Álvarez Rigaudias, 2012).

Por otro lado, Piñar Mañas (2019) subraya que el art. 49.1.g) RGPD, aporta una interesante precisión cuando reconoce la licitud de las transferencias realizadas desde un registro público que, de acuerdo con el Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, siempre

ciente y deliberadamente según Coudray (2004), el Alto Tribunal de la Unión limitó el ámbito de aplicación de la Directiva 95/46/CE atendiendo a las características técnicas de internet, considerando inaplicables al caso de autos las previsiones sobre transferencia de datos personales a terceros países. De este modo, la consulta de datos personales a través de internet no fue considerada una transferencia internacional de datos personales[7].

c) La transferencia de datos personales no debe tener por objeto ninguna de las actividades relacionadas como excepciones del ámbito de aplicación del RGPD (art. 2.2), entre las que se encuentra el tratamiento de datos personales por parte de autoridades competentes con fines de prevención, investigación, detección, enjuiciamiento o ejecución de infracciones penales, incluida la protección frente amenazas a la seguridad pública y su prevención [letra d)].

En relación con esta excepción, deben tomarse en consideración los decisivos pronunciamientos del TJUE sobre los acuerdos relativos a la trans-

---

que en la consulta se cumplan las garantías del Derecho de la Unión o de los Estados miembros. Una regulación que, como se puede apreciar, tiene como base de la licitud la "puesta a disposición de los datos para su consulta" y no el "envío de la información" (p. 433).

[7] En efecto, el Alto Tribunal de la UE ha tratado de acotar territorialmente el marco de vigencia de la normativa europea sobre protección de datos personales al ámbito de la Unión teniendo en cuenta tres aspectos:

En primer término, el hecho de que internet constituye una red mundial sin fronteras donde los motores de búsqueda confieren carácter ubicuo a la información y a los enlaces contenidos en una lista de resultados (TJUE asunto *Google Spain y Google*, 2014, par. 80 y asunto *Bolagsupplysningen e Ilsjan*, 2017, par. 48), de manera que, aunque los internautas que se encuentran fuera de la Unión pueden acceder a un enlace que remite a una información cuyo centro de interés se sitúa en la Unión, ello no implica que el legislador de la Unión sea competente para imponer obligaciones al gestor de un motor de búsqueda situado fuera del territorio de la Unión.

En segundo lugar, se toma en consideración que el derecho a la protección de datos personales no constituye un derecho absoluto, sino que debe ser considerado manteniendo una relación de proporcionalidad con otros derechos fundamentales [TJUE asunto *Volker und Markus Schecke y Eifert* (2010), par. 48], y el Dictamen 1/15 (2017) sobre el *Acuerdo PNR UE-Canadá* (par. 136).

En última instancia, se valora la circunstancia de que la ponderación entre los derechos al respeto de la vida privada y a la protección de datos personales de un lado, y la libertad de información de los internautas de otro, puede plantearse con variaciones sustanciales en los distintos terceros Estados.

La reciente sentencia del TJUE en el asunto *Google LLC* –que se subroga en los derechos de Google Inc.- *v. Commission nationale de l'informatique et des libertés (CNIL)* (2019), ha considerado que ni del tenor de la Directiva 95/46/CE ni del RGPD puede deducirse que se pueda exigir al gestor de un motor de búsqueda en la Unión Europea, que proceda a la retirada de enlaces en todas las versiones de su motor cuando haya estimado una solicitud de retirada de enlaces presentada por un interesado (pars. 64-65).

Acerca de la importancia de la aplicación extraterritorial de la normativa europea de protección de datos *vid.*, entre otros, Gömann (2017) y Zhao y Chen (2019).

ferencia de registros de datos personales de los pasajeros (*Passenger Name Record-PNR*)[8].

Así, en el asunto *Parlamento Europeo v. Consejo y Comisión* (2006) el TJUE no solo anuló la Decisión de 17 de mayo, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional (Oficina de aduanas y protección de fronteras de los Estados Unidos —*United States Bureau of Customs and Border Protection*— CBP), sino también la Decisión de 14 de mayo de 2004 sobre el carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren a la Oficina de aduanas y protección de fronteras de los Estados Unidos[9].

Idéntica suerte corrió, aunque por otra vía, el acuerdo sobre la transferencia de registros de datos personales de los pasajeros (*Passenger Name Record*-PNR) firmado el 25 de junio de 2014 entre la UE y Canadá, cuyo art. 3.1 preveía que las Partes convenían en que los datos API/PNR referentes a viajeros serían objeto de tratamiento por la *Canadá Border Services Agency* (CBSA). A través del Dictamen 1/15 (2017) emitido con arreglo al art. 218 TFUE a petición del Parlamento Europeo, el Tribunal de Justicia declaró que dicho Acuerdo no podía ser firmado en la versión que le había sido remitida debido a la incompatibilidad de varias de sus disposiciones con los derechos reconocidos en los arts. 7, 8 y 52.1 CDFUE, que "se oponen tanto a la transferencia de datos sensibles" como al "uso y conservación" de los mismos por las autoridades de un país tercero (par. 167)[10].

---

[8] Un análisis exhaustivo de la Sentencia y del Dictamen del TJUE se encuentra en Pérez Francesch *et al. (2011)*.

[9] En opinión del Alto Tribunal de la Unión Europea, la transferencia internacional de datos que autorizaban dichas Decisiones no puede ampararse en la Directiva 95/46/CE por no ser de aplicación al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal (pars. 55 y 59). Sin embargo, como afirmara en su momento Mendez (2007), el "drama" del acuerdo del PNR entre la UE y los Estados Unidos estaba lejos de concluir habida cuenta de los intereses en juego, entre ellos, no solo la adecuada ponderación entre la seguridad y la libertad personal en un sistema democrático, sino también, las consecuencias económicas para las compañías aéreas europeas (p. 147).

[10] Para ser compatible con la CDFUE a juicio del Tribunal de Justicia el Acuerdo PNR entre la UE y Canadá debía, en primer término, garantizar que la utilización y comunicación de esos datos a otras autoridades salvo casos de urgencia debidamente justificados, se somete a un control previo efectuado por un órgano judicial o una entidad administrativa independiente que se pronuncie a raíz de una solicitud motivada de esas autoridades.

También resultaba indispensable según afirmaba, que dicho Acuerdo PNR contemplara la limitación de la conservación de los datos tras la partida de los pasajeros aéreos, a los de aquellos pasajeros respecto de los que existan elementos objetivos que permitan considerar la posibilidad de que presenten un riesgo en materia de lucha contra el terrorismo y los delitos graves de carácter transnacional.

Como se podrá apreciar en las páginas que siguen, los pronunciamientos del TJUE en los asuntos *Schrems I* y *Schrems II* en relación con los instrumentos jurídicos articulados para llevar a cabo las transferencias de datos personales desde la UE a los Estados Unidos, toman en consideración algunas de las garantías aplicables a los acuerdos PNR que la Unión ha intentado suscribir con los EEUU y Canadá. En todo caso, conviene aclarar con carácter previo cuáles son los instrumentos de licitud de las transferencias internacionales de datos en el ordenamiento europeo y qué tipo de excepciones se prevén.

1.2. Instrumentos de licitud de las transferencias internacionales de datos en el ordenamiento europeo

La aplicación obligatoria en los Estados miembros del RGPD desde el 25 de mayo de 2018, ha supuesto la introducción de cambios sustantivos en la normativa de protección de datos de la UE. Esta nueva regulación europea resulta mucho más compleja que la Directiva 95/46/CE[11], incorporando prin-

---

Asimismo, el TJUE consideraba que el citado Acuerdo PNR debía supeditar la comunicación de los datos del PNR a las autoridades públicas de un país tercero al requisito de que exista un Acuerdo entre la UE y ese país tercero, o bien una decisión adoptada por la Comisión relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos que incluya la identificación de las autoridades a las que se prevea comunicar los datos de los pasajeros.

Actualmente, la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuicia-miento de los delitos de terrorismo y de la delincuencia grave, regula de modo específico y proporcionado según Lowe (2016) la transferencia por las compañías aéreas de datos del registro de nombres de los pasajeros (PNR) de vuelos exteriores de la UE [art. 1.a)], que podrán tratarse únicamente con fines de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y los delitos graves contemplados en el artículo 6, apartado 2, letras a), b) y c) (art. 1.2).

[11] En efecto, entre las novedades de mayor calado que contempla el RGPD se suele mencionar la consagración del principio de la "privacidad desde el diseño y por defecto" (art. 25 RGPD), como concreción de la denominada "responsabilidad proactiva" (*accountability*). Esta última ha sido definida por el Grupo de Trabajo del Art. 29 en su Documento (WP 168, p. 19), como la exigencia a los responsables del tratamiento de que implementen "las medidas necesarias para asegurar que los principios básicos y las obligaciones de la actual Directiva sean respetados al tratar datos personales". Unas exigencias que el nuevo RGPD también asigna, en mayor medida que la Directiva 95/46/CE, no solo a los responsables sino también a los encargados del tratamiento (Voss, 2016, p. 222).

Desde tales premisas, la protección de datos desde el diseño y por defecto consiste en la obligación del responsable del tratamiento de adoptar entre otras, medidas tales como la reducción al máximo del tratamiento de datos personales, la rápida "seudonimización" de los datos personales, la adopción de medidas de transparencia en las

cipios de la protección de datos relacionados con las transferencias internacionales que no habían sido tomados en consideración anteriormente por el legislador comunitario como la privacidad desde el diseño y por defecto, considerada una de las novedades del RGPD en el contexto del cambio de paradigma respecto a la regulación europea anterior.

Aunque según afirma la Comisión Europea en su Comunicación de 10 de enero de 2017, en relación con las transferencias internacionales de datos "la arquitectura sigue siendo, en esencia, la misma que dispuso la Directiva de 1995" (COM, 2017a, p. 4), el RGPD también lleva a cabo una reforma de las normas relativas a las transferencias internacionales, aclarando y simplificando su utilización e introduciendo nuevos instrumentos de transferencia[12].

En consecuencia, el principio general por el que se rigen las transferencias internacionales de datos aparece reconocido en el art. 44 RGPD, exigiendo —tanto al responsable como al encargado del tratamiento de los datos personales en el tercer país, así como a las posibles transferencias ulteriores de datos desde allí—, el cumplimiento de determinadas condiciones con el fin de que el nivel de protección de las personas físicas garantizado por la norma europea no se vea menoscabado.

Al igual que la Directiva 95/46/CE, el RGPD valida las transferencias internacionales de datos personales a partir del concepto de protección sustancialmente equivalente en el tercer país u organización internacional a la otorgada en el ordenamiento de la Unión Europea[13]. Desde esta premisa, incorpora nuevos instrumentos de licitud con respecto a los previstos en la Directiva 95/46/CE pero también, como se comprobará a continuación, prevé una nueva excepción aplicable a situaciones específicas que genera importantes dudas jurídicas.

---

funciones y el tratamiento de datos personales que permita a los interesados supervisar el tratamiento de sus datos (RGPD, Cond. 30).

[12] El interés del legislador europeo por aportar mayor precisión a la regulación de las transferencias internacionales de datos se evidencia en términos estrictamente cuantitativos por la extensión que el RGPD dedica a su regulación (siete artículos), frente a los dos preceptos que dedicaba a esta materia la anterior Directiva 95/46/CE. Una regulación más amplia que en opinión de Piñar Mañas (2016) pone de manifiesto la conciencia de la importancia de esta materia en un mundo globalizado junto a la voluntad de proporcionar "reglas más claras" sobre la materia (p. 428).

En todo caso, cabe reseñar también el hecho de que desde la entrada en vigor de la Directiva 95/46/CE a la adopción en 2016 del RGPD, el TJUE ha tenido ocasión de pronunciarse en diversas ocasiones sobre diferentes aspectos de las transferencias internacionales de datos, incorporando a través de sus resoluciones importantes explicaciones y precisiones que han sido incorporadas a la legislación europea.

[13] Atendiendo a la definición del art. 4 (26) RGPD, "organización internacional" hace referencia a una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países.

1.2.1. Transferencias mediante decisiones de adecuación

Si bien el medio general para la transferencia de datos personales a terceros países sigue siendo la decisión de adecuación, el art. 45.2 RGPD ofrece un catálogo preciso y detallado de los aspectos a tomar en consideración por la Comisión a la hora de evaluar el grado de aproximación a las garantías establecidas en la UE por parte del ordenamiento jurídico de un tercer país o de una organización internacional.

De acuerdo con el apartado 2 del art. 45 RGPD y la interpretación realizada por el TJUE en el asunto *Schrems I* en 2015, donde reconoció que el principio de adecuación no exige que el ordenamiento jurídico del tercer país interesado reproduzca literalmente las normas de la UE (par. 74), la Comisión tendrá en cuenta en su evaluación la existencia en el ordenamiento jurídico del tercer país de determinadas garantías aplicables con carácter general al conjunto de los derechos fundamentales y, en particular, a la protección de datos personales.

Así, entre otros aspectos, el citado precepto del RGPD prevé que la Comisión evaluará en el tercer país la vigencia del Estado de Derecho, el respeto de los derechos humanos y de las libertades fundamentales, la legislación en materia de protección de datos y las normas conexas relativas a seguridad nacional, la legislación penal, el acceso de autoridades públicas a datos personales, las normas profesionales, las medidas de seguridad (incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional), la jurisprudencia, los recursos administrativos y las efectividad de las acciones judiciales para los interesados.

La Comisión también tomará en consideración la existencia y funcionamiento efectivo en el tercer país de una o varias autoridades de control independientes, sus funciones de ejecución normativa, la responsabilidad en el cumplimiento normativo que dicha autoridad tiene asignada, las medidas de asistencia y de asesoramiento a los interesados encomendadas, y la previsión de cooperación con las autoridades de control de la UE y de los Estados miembros.

En última instancia, serán objeto de valoración por la Comisión los compromisos internacionales asumidos por el tercer país u organización internacional (en especial, su adhesión al Convenio núm. 108 y a su Protocolo adicional adoptados en 1981 por el Consejo de Europa modernizado en 2018), otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes y su participación en sistemas multilaterales o regionales en materia de protección de datos.

Aun cuando las decisiones de adecuación constituyen "documentos 'vivos'" (COM, 2017a, p. 10) que deben ser supervisados de manera continuada por la Comisión y adaptados en caso producirse acontecimientos que afecten al nivel de protección garantizado por el tercer país en cuestión (art. 45.4 y 5 RGPD), como afirma Gonzalo Domenech (2019), en el contexto de las garan-

tías proporcionadas por la normativa de la Unión constituyen el instrumento jurídico más "seguro" para transferir datos a terceros Estados u Organizaciones internacionales (p. 352).

1.2.2. Otros instrumentos lícitos de transferencias internacionales de datos personales

A falta de una decisión de adecuación, la nueva normativa (art. 46.2 RGPD) mantiene la posibilidad de que las transferencias internacionales puedan basarse en instrumentos alternativos que ofrezcan también garantías adecuadas.

Entre tales mecanismos se prevé la transferencia internacional de datos personales a través de "un instrumento jurídicamente vinculante y exigible entre las autoridades y organismos públicos" [art. 46.2, letra a)], lo que equivale a reconocer -junto a los acuerdos administrativos entre autoridades y organismos públicos autorizados por la autoridad de control competente previstos en el art. 46.3.b)-, la licitud de transferencias internacionales de datos personales a través de instrumentos y acuerdos internacionales de carácter multilateral o bilateral (CEPD-EDPB, 2020, par. 10).

Aunque la forma jurídica del convenio no resulta determinante siempre que sea legalmente vinculante y susceptible de aplicación, el CEPD-EDPB ha concretado unas recomendaciones generales que prevén la incorporación de cláusulas relativas a los fundamentos (pars. 15-16), principios (pars. 15-26) y derechos de los interesados en la protección de datos (pars. 27-39), equivalentes a las previstas por la normativa europea interpretada según la jurisprudencia del TJUE.

Estas recomendaciones generales también incluyen limitaciones respecto de transferencias ulteriores e intercambio de datos incluyendo previsiones relativas a la divulgación y acceso de las autoridades gubernamentales (pars. 41-48), y mecanismos eficaces de reparación y de supervisión (pars. 50-63).

También se podrán realizar transferencias internacionales de datos personales al amparo del art. 46.2 RGPD mediante "cláusulas tipo" ("cláusulas contractuales tipo" en la terminología de la Directiva 95/46/CE), adoptadas por la Comisión o por la autoridad de control y posteriormente aprobadas por la Comisión [letras c) y d)]; "códigos de conducta" o "mecanismos de certificación" (como sellos y marcas de privacidad) acompañados de compromisos vinculantes exigibles al responsable o al encargado del tratamiento de datos en el tercer país de cumplir las garantías adecuadas [letras e) y f)], y "normas corporativas vinculantes" [letra b)][14].

[14] Las normas corporativas vinculantes se adoptaban hasta la aplicación efectiva del RGPD entre entidades pertenecientes a un mismo grupo empresarial, pero la nueva regulación europea permite que sean acordadas por un grupo de empresas de-

Además de los acuerdos administrativos entre autoridades y organismos públicos a los que anteriormente se hacía referencia, el art. 46.3, letra a) prevé también la licitud de las transferencias internacionales de datos personales mediante "cláusulas contractuales" entre el responsable o encargado en el país de origen de la transferencia y el responsable o encargado de los datos en el tercer país.

1.2.3. Excepciones para las transferencias internacionales de datos en situaciones específicas

También aparecen reguladas en el art. 49 RGPD las denominadas "excepciones para situaciones específicas" aplicables en ausencia de una decisión de adecuación o de otras garantías adecuadas.

Ante la concurrencia de dicha circunstancia, la transferencia internacional de datos personales será lícita si media el consentimiento explícito del interesado [art. 49.1.a)]; la transferencia resulta necesaria para la celebración o ejecución de un contrato [art. 49.1.b) y c)]; concurren razones importantes de interés público [art. 49.1.d)]; la transferencia es necesaria para el ejercicio de una acción de reclamación [art. 49.1.e)]; el objeto de la transferencia viene constituido por la protección de intereses vitales del interesado o de otras personas física o jurídicamente incapacitados para prestar su consentimiento [art. 49.1.f)], o la transferencia se realice desde un registro público que tenga por objeto facilitar información al público o persona singular que acredite un interés legítimo, siempre que, en cada caso particular, se garantice el cumplimiento del Derecho de la Unión o del Estado miembro respecto de la consulta [art. 49.1.g)].

No obstante, la enumeración de las excepciones no concluye con los supuestos enumerados en el primer párrafo del apartado 1 del art. 49 RGPD. Es el segundo párrafo de dicho precepto el que prevé la excepción que más dudas jurídicas plantea, calificada por Castellanos Rodríguez (2017) como un "cajón de sastre" que "contradice, *a priori*" las intenciones de maximizar las garantías que pretende la norma europea al permitir que las transferencias de datos personales puedan tener lugar en aras de los "intereses legítimos imperiosos" de una determinada empresa (p.12).

La falta de concreción de la expresión "intereses legítimos imperiosos" genera numerosas dudas acerca de las transferencias internacionales a las

---

dicado a una "actividad económica conjunta" –concepto que requiere de una concreción por parte del legislador- sin necesidad de pertenecer al mismo grupo empresarial [art. 46.2, b) y art. 47 RGPD].

Por su parte, el Comité Europeo para la Protección de Datos (CEPD-EDPB) ha creado un registro on-line en el que se publican las decisiones adoptadas por las autoridades de control de los Estados miembros respecto de las normas corporativas vinculantes. Disponible en: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_es (última visita: 14 de sept. de 2020).

que ofrecería cobertura legal, a pesar de que el Considerando 113 RGPD hace referencia en relación con este concepto al hecho de que deben ser tomadas en consideración "las legítimas expectativas" de la sociedad en un aumento del conocimiento para "fines de investigación científica o histórica o fines estadísticos".

En todo caso, el Considerando antes citado subraya que este supuesto únicamente puede utilizarse "en casos aislados" y detalla ciertos requisitos que deben concurrir para poder llevar a cabo este tipo de transferencias. Así, el exportador de datos debe atender especialmente a la naturaleza de los datos personales, la finalidad y la duración de la operación, el tipo de las operaciones de tratamiento propuestas, las garantías de protección de los derechos fundamentales y las libertades públicas con respecto al tratamiento de datos de los interesados en el país de origen, en el tercer país, y en el país de destino final.

Junto a la dicción del párrafo segundo del art. 49.1 RGPD y a las indicaciones contenidas en el Considerando 113 RGPD, resulta especialmente destacable el esfuerzo de las Directrices 2/2018 del Comité Europeo de Protección de Datos (CEPD-EDPB) por concretar lo que debe entenderse por "casos aislados" para la utilización lícita de este instrumento de transferencia.

En efecto, el CEPD-EDPB opta por una aplicación restrictiva de las excepciones contempladas en el párrafo segundo del art. 49.1 RGPD considerando que, en virtud del principio de responsabilidad, tanto el responsable y el encargado del tratamiento como el exportador de datos, deben "poder demostrar que no era posible" la transferencia de datos con garantías adecuadas de acuerdo con el art. 46 RGPD, ni la aplicación de ninguna de las excepciones previstas en el art. 49.1 párrafo primero RGPD mediante la realización de "serios intentos" en este sentido. Asimismo, como "requisito adicional", afirma, ha de realizarse una "prueba de ponderación" del interés legítimo imperioso perseguido por el exportador de datos y de los intereses o los derechos y libertades del interesado.

Del mismo modo, cabe subrayar la relevancia de la distinción que lleva a cabo el CEPD-EDPB entre "intereses legítimos" e "intereses imperiosos" aplicando una interpretación restrictiva respecto de estos últimos, a los que exige un "umbral superior" de limitación, aunque sin concretar los elementos que deben ser tomados en consideración en su valoración.

En última instancia, el Comité Europeo de Protección de Datos también precisa en estas Directrices dos aspectos relevantes. De un lado, que la obligación de informar a la autoridad de supervisión respecto de este tipo de transferencias no significa que "deba(n) ser autorizada(s) por la autoridad de supervisión" (se trata, pues, de ponerlas en conocimiento de la autoridad de supervisión) y, de otro, que la obligación de suministrar al interesado información acerca de los intereses imperiosos perseguidos constituye una obligación adicional a la información que, con carácter general, se le debe facilitar según el tenor de los arts. 13 y 14 RGPD (CEPD-EDPB, 2018, pp. 16-17).

2. EL PRIMER INSTRUMENTO DE ADECUACIÓN DE LAS TRANSFERENCIAS TRANSATLÁNTICAS UE-EEUU: EL PUERTO SEGURO (*SAFE HARBOR*)

2.1. Las carencias originales del sistema de Puerto Seguro

Tomando en consideración la importancia de los flujos de datos transfronterizos entre la UE y los EEUU, con la entrada en vigor de la Directiva 95/46/CE la UE y los EE.UU adoptaron una decisión de adecuación sobre la que posteriormente se sustentaría el acuerdo de Puerto Seguro (*Safe Harbor*), garantizando teóricamente que las transferencias de datos personales a uno y otro lado del Atlántico se llevaban a cabo con unas garantías de protección equivalentes a las adoptadas por el ordenamiento europeo.

Así, atendiendo al criterio dispuesto por el art. 25 de la Directiva 95/46/CE, según el cual el nivel de protección adecuado (*adequate level of protection*) de los datos objeto de transferencia a un tercer país debe evaluarse caso por caso y, por lo tanto, tomando en consideración todas las circunstancias que concurren en la misma, el Grupo de Trabajo de protección de las personas en lo que respecta al tratamiento de datos personales, publicó unas directrices para la elaboración de las evaluaciones de adecuación (WP 12, 1998) en concordancia con las previsiones contempladas hasta entonces en el Convenio 108 del Consejo de Europa.

En opinión del Grupo de Trabajo, partiendo de la Directiva 95/46/CE y tomando en consideración todas las regulaciones internacionales, es posible enunciar un "núcleo duro" de la protección de datos que, sin carácter inamovible, define el contenido, el procedimiento y la aplicación de lo que puede ser entendido como un mínimo común respecto del nivel de protección adecuado.

Como principios básicos definidores del concepto de protección adecuada, el Grupo de Trabajo enunciaba:

— El principio de limitación de los fines (*purpose limitation principle*), en virtud del cual, los datos deben ser procesados con una finalidad específica y, en consecuencia, únicamente pueden ser transferidos en el marco de dicha finalidad. Las excepciones a este principio vienen constituidas por los supuestos previstos en el art. 13 Directiva 95/46/CE, donde se prevén aquellos relativos a la seguridad nacional, a la prevención, investigación, detección y enjuiciamiento de delitos o infracciones en la deontología en las profesiones reguladas, a la concurrencia de un importante interés económico o financiero, y a la protección de los datos personales de un sujeto o de los derechos y libertades de otros.

— El principio de la calidad y proporcionalidad de los datos (*data quality and proportionality*), que exige que los datos sean exactos y, en su caso, estén actualizados y sean adecuados para el propósito del tratamiento.

— El principio de transparencia (*transparency principle*), según el cual se debe proporcionar a los interesados información acerca del objeto del procesamiento y de la identidad del responsable del tratamiento en el tercer país. Las excepciones a este principio hacen referencia al tratamiento con fines estadísticos o de investigación histórica o científica, a la imposibilidad fáctica de informar a los interesados, o al hecho de que el registro o la comunicación a un tercero esté prevista por la ley (arts. 13 y 11.2 Directiva 95/46/CE).

— El principio de seguridad de los datos (*security principle*), que exige al responsable del tratamiento de datos la adopción de las medidas de seguridad necesarias atendiendo a los riesgos que entrañe el tratamiento.

— Los derechos de acceso, rectificación y oposición (*rights to access, rectification and opposition*), que implican el derecho del interesado a tener una copia de todos los datos objeto de procesamiento referidos a su persona, el derecho de rectificación de los que sean inexactos y, en determinadas circunstancias, a oponerse a su tratamiento.

— El derecho a la restricción de ulteriores transferencias (*restrictions on onward transfers*), que impide posteriores transferencias de datos por el primer receptor si los subsiguientes no cumplen los requisitos exigidos por el nivel de protección adecuado.

Además, desde la perspectiva del procedimiento y la aplicación de la protección de datos a las transferencias de datos personales el Grupo de Trabajo consideraba que una protección adecuada implicaba, en primer término, ofrecer un buen nivel de cumplimiento de las normas (*good level of compliance*).

El buen nivel de cumplimiento de las normas se alcanzaba, a su juicio, mediante el desarrollo de una elevada concienciación de las obligaciones que competen a los responsables del tratamiento, a través de la previsión de sanciones efectivas y disuasorias frente a incumplimientos, y de la facilitación de apoyo y ayuda a los interesados en el ejercicio de sus derechos (*support and help to individual data subjects*).

Este apoyo y ayuda a los interesados, afirmaba el Grupo de Trabajo, podía llevarse a cabo gracias a la articulación de instrumentos que proporcionaran una tutela rápida y efectiva sin un coste económico prohibitivo, junto a la garantía de una reparación adecuada (*appropriate redress*) a la parte perjudicada en casos de incumplimiento de las normas garantizadas. A tales efectos, consideraba idónea la existencia de algún tipo de institución que lleve a cabo una investigación independiente de las reclamaciones (WP 12, 1998, pp. 5-7).

Poco después, en el año 1999, la Comisión Europea y el Departamento de Comercio de los Estados Unidos alcanzaron el Acuerdo de Puerto Seguro (conocido como *Safe Harbor*), con el fin de posibilitar que las empresas de los Estados Unidos se adhiriesen a determinados principios que garantizaban la

aplicación de los estándares europeos de protección de datos personales en las transferencias de datos personales[15].

Dictaminado en un primer momento por el Grupo de Trabajo del art. 29 (WP 32, 2000), este órgano reconocía que atendiendo al art. 1 de la Directiva 95/46/CE y al Convenio Europeo de los Derechos Humanos, el acuerdo de Puerto Seguro garantizaba la tutela por órganos independientes del derecho a la intimidad (*Right to Privacy* en su acepción anglosajona, y derecho a la vida privada o a la privacidad en la Europa continental) como derecho "fundamental"[16].

---

[15] Como afirma Lam (2017, p. 4), el marco de adecuación del Puerto Seguro (*Safe Harbor*) es un procedimiento ágil para dar cumplimiento a las garantías exigidas por la legislación europea en las transferencias internacionales de datos personales, pero no el único pues, como se ha mencionado anteriormente, existen mecanismos alternativos como las cláusulas contractuales tipo o cláusulas tipo y las normas corporativas vinculantes, previstos tanto en la Directiva 95/46/CE como en el actual RGPD.

[16] Aun cuando la identificación del derecho a la protección de datos como derecho autónomo no resulta una cuestión pacífica en la doctrina, la Carta de los Derechos fundamentales de la Unión Europea (art. 8) y la Constitución española (art. 18.4 CE) —según la interpretación del Tribunal Constitucional español en las Sentencias TC 292/2000 y 254/1993—, le otorgan sustantividad propia.

También en el ámbito del Consejo de Europa se adoptó en 1981 el ya mencionado Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE núm. 108) recientemente modificado, y el TEDH incluyó la protección de datos personales entre los elementos garantizados por el art 8 CEDH en los asuntos *Amann v.Switzerland* (2000) y *Rotaru v. Romania* (2000).

En el caso de la CDFUE, el TJUE tuteló el derecho a la vida privada y familiar (art. 7) y a la protección de datos de carácter personal (art. 8), en el asunto *Rijkeboer* (2009).

Por su parte, el TC ha reconocido que, en el ámbito de la informática y el progreso tecnológico, el derecho fundamental a la intimidad (art. 18.1 CE) no aporta "por sí solo una protección suficiente", *lo que explica que el constituyente incorporara en el art. 18.4 CE "un* «instituto de garantía» como medida de protección frente a la amenaza para la dignidad y los derechos de la persona que es también, en sí mismo, "«un derecho o libertad fundamental»" (STC 254/1993. FJ. 6). Un derecho fundamental a través del cual el constituyente trataba de proporcionar "no solo un ámbito de protección más específico sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el apartado 1 del precepto" (STC 292/2000. FJ. 4).

En efecto, suele ser común reconocer que el origen del derecho a la privacidad (*Right to Privacy)* entendido como "autodeterminación informativa" (*Recht auf informationelle Selbstbestimmung*) se sitúa en la Sentencia del Tribunal Constitucional Federal alemán de 15 de diciembre de 1983 asunto Ley del Censo, donde se enuncia en el contexto de la protección de los derechos de la personalidad y es definido como el derecho del individuo a decidir sobre la "divulgación y uso de sus datos" (par. 147), al tiempo que se reconocen los riesgos para los derechos de la personalidad derivados de las "redes de datos" o "datos enmallados" (*Datenverbundes*) (par. 169).

A este respecto, véase, Lucas Murillo de la Cueva (1990) y (2003).

Unas reflexiones exhaustivas de diferentes autores acerca de los orígenes, la regulación normativa y las problemáticas recientes y previsibles en un futuro próximo en

Sin embargo, dicho dictamen también puso de manifiesto significativas debilidades y carencias presentes todavía en la última versión del acuerdo *Safe Harbor* de transferencia de datos personales entre la UE y los EEUU.

Entre las primeras, el Grupo de Trabajo subrayaba el hecho de que la adhesión al sistema de Puerto Seguro se basaba en la "autocertificación" de las propias empresas sin ningún tipo de verificación previa por organismos públicos. Una práctica que, en su opinión, restaba credibilidad al acuerdo[17]. Entre las segundas, cabe destacar la advertencia acerca del uso "restrictivo y controlado" que debía hacerse de las excepciones, cuya utilización no debía suponer un debilitamiento de los principios de protección por las autoridades norteamericanas incompatible con la Directiva europea.

El análisis exhaustivo del Acuerdo de Puerto Seguro llevó al Grupo de Trabajo a concluir que el mecanismo de ejecución contemplado en el mismo resultaba deficiente, debiendo mejorarse en los aspectos relativos a la facilitación de apoyo y ayuda a los interesados, así como mediante la previsión de un resarcimiento adecuado a la parte perjudicada cuando se produjera un incumplimiento de las normas (WP 32, 2000, pp. 3-7).

Tales observaciones no impidieron que el 26 de julio de 2000 la Comisión Europea adoptara la Decisión 2000/520/CE, donde reconoce que la protección de datos en el marco del Puerto Seguro garantizaba un nivel de protección adecuado para los datos transferidos desde la Unión Europea a los Estados Unidos sin necesidad de establecer ninguna garantía adicional. No obstante, el tiempo demostraría, en opinión de Svantesson (2016), que la estructura del Puerto Seguro estaba "construida sobre la arena" (p. 39).

2.2. El Puerto Seguro (*Safe Harbor*) ante el Tribunal de Justicia: la Sentencia *Schrems I*

Las insuficiencias en la seguridad del sistema de Puerto Seguro hicieron saltar las alarmas en las instituciones europeas cuando en junio de 2013 las revelaciones de E. J. Snowden a los diarios *The Guardian* y *The Washington Post* alertaban de operaciones de vigilancia masiva llevadas a cabo por la Agencia de Seguridad Nacional norteamericana (NSA por sus siglas en inglés).

Dichas informaciones supusieron el inicio de una investigación por parte del Parlamento Europeo que concluyó con la Resolución de 12 de marzo de

---

relación con el derecho a la protección de datos personales en las sociedades actuales, se han publicado en la sección "Encuesta sobre la protección de datos" (VVAA, 2020).

[17] En efecto, el acuerdo *Safe Harbor* entre la UE y los Estados Unidos preveía que las compañías norteamericanas se autocertificasen ante la *Federal Trade Commission (FTC)* y se adhirieran a los principios de protección que protegían los flujos de datos transatlánticos pero, en la práctica, según afirman Ustarán y García (2019), las empresas adheridas "no realizaban sus revisiones anuales y siempre existió una falta de coerción por parte de la FTC en comparación con otros asuntos domésticos" (p. 465).

2014 (PE 2014) en la que reprobaba "la recopilación generalizada extensa y sistemática de los datos personales", llamando la atención sobre el hecho de que "los sistemas de vigilancia masiva indiscriminada por parte de los servicios de inteligencia constituyen una seria injerencia en los derechos de los ciudadanos", y condenando "firmemente" que servicios de inteligencia extranjeros "hayan intentado rebajar los estándares de seguridad informática" (PE 2014, pars. 10, 92).

Finalmente, en la Comunicación [COM(2013) 847 final] la Comisión Europea reconoció que, según constataba el Grupo de Trabajo *ad hoc* EU-EEUU sobre protección de datos, las garantías adoptadas por la legislación estadounidense no contemplaban los derechos de acceso, rectificación y cancelación de los datos personales ni a ciudadanos estadounidenses ni a europeos (COM, 2013a, pp. 18-19).

Por otro lado, la Comisión constató que entre las compañías certificadas se encontraban empresas de red como Google, Facebook, Microsoft, Apple o Yahoo, beneficiarias de un amplísimo número de usuarios en Europa que podían no tener conocimiento del tratamiento de sus datos personales transferidos a los EEUU, habida cuenta de que dichas entidades no comunicaban la aplicación de excepciones a los principios de Puerto Seguro. Además, el supuesto concreto del acceso a gran escala por las agencias de inteligencia a los datos personales transferidos bajo el sistema de Puerto Seguro, cuestionaba gravemente el derecho de los europeos a la protección de datos[18].

Al mismo tiempo, en la Comunicación [COM(2013) 846 final] de la misma fecha que la anterior, la Comisión reconocía que el Puerto Seguro constituía un componente importante de las relaciones comerciales de la UE y los Estados Unidos de modo que, según afirmaba, la crisis de confianza podía supe-

[18] De hecho, existe un tratamiento generalizado de datos por parte de las agencias de inteligencia de los Estados integrados en la organización conocida como "Los Cinco Ojos" (*Five Eyes- FVEY*) compuesta por los EEUU., Reino Unido, Canadá, Australia y Nueva Zelanda, a la que se han incorporado a través de acuerdos bilaterales con Estados Unidos algunos Estados miembros de la UE como Francia y Alemania (Kuner, 2017, p. 899). Pero también entre los integrantes de programas más amplios como "Nueve Ojos" (*9-Eyes*) y "Catorce Ojos" (*14-Eyes*), que incluyen a Dinamarca, Países Bajos, Francia, Alemania, Bélgica, Italia, España y Suecia) (Roth, 2017, p. 64).

Respecto de los dos últimos programas el Parlamento Europeo afirmó en su Resolución de 12 de marzo de 2014, que pesa sobre los Estados miembros que participan en los denominados programas "Nueve Ojos" y "Catorce Ojos", la obligación de evaluar y revisar, si fuera necesario, su legislación nacional y las prácticas desarrolladas por los servicios de inteligencia con el fin de "asegurar" que respetan los "principios de legalidad, necesidad, proporcionalidad, garantías debidas, información al usuario y transparencia", incluido el cumplimiento de la recopilación de buenas prácticas de Naciones Unidas y las recomendaciones de la Comisión de Venecia. Asimismo, deberán garantizar el cumplimiento de los estándares de la Convención Europea de los Derechos Humanos, los respectivos derechos fundamentales del Estado miembro de que se trate y, en particular, aquellos relativos a la protección de datos, la privacidad y la presunción de inocencia (PE, 2014, p. 46).

rarse mediante una renegociación que restableciera las deficiencias y lo hiciera más seguro, a través de la incorporación de trece recomendaciones que formulaba en la Comunicación [COM(2013) 847 final] (COM, 2013b, pp. 7-8).

Estas recomendaciones se centraban en aspectos tales como garantizar la transparencia, la incorporación de sistemas de solución extrajudicial de controversias asequibles y de fácil acceso para los usuarios, la supervisión e investigación de las autocertificaciones, el cumplimiento de los principios del Puerto Seguro, y el acceso a los datos personales transferidos por parte de las autoridades estadounidenses. En relación con esta última cuestión, se preveía que "la excepción relativa a la seguridad nacional prevista en la Decisión de puerto seguro no se utilice más allá de lo estrictamente necesario o proporcionado" (COM, 2013a, p. 21)[19].

Además, los efectos de las revelaciones de E. J. Snowden a los medios de comunicación difundidas mundialmente fueron más allá del limitado reconocimiento por las instituciones europeas de las deficiencias del sistema de Puerto Seguro, situando la cuestión en sede jurisdiccional a raíz del planteamiento de una reclamación dirigida contra Facebook Ireland, filial de Facebook Inc. (esta última con sede en los EEUU) por parte del Sr. Schrems, ciudadano austriaco y usuario de la red social Facebook el 25 de junio de 2013, en la que solicitaba el cese de la transferencia de sus datos personales a EEUU.

A partir de este momento, el curso de la reclamación del Sr. Schrems va a coincidir en el tiempo con la negociación entre la Comisión Europea y las autoridades estadounidenses dirigida a reforzar el modelo de Puerto Seguro que, como se verá a continuación, concluyó con la adopción de un nuevo instrumento de licitud para las transferencias de datos personales entre la UE y los EEUU denominado Escudo de Privacidad (*Privacy Shield*).

En efecto, tras el rechazo por parte de la autoridad de control irlandesa a investigar la queja formulada por el Sr. Schrems por considerarla infundada, esta fue convertida en recurso ante el Tribunal Superior irlandés (*High Court*) y este órgano jurisdiccional no solo la admitió a trámite sino que consideró

---

[19] En el asunto *Digital Rights Ireland y otros (*2014) el Tribunal de Justicia de la Unión Europea declaró inválida la Directiva 2006/24/CE sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, al estimar que la conservación de datos para su posterior acceso por las autoridades nacionales competentes que preveía, aun respondiendo al objetivo de interés general de la prevención de delitos y la lucha contra la delincuencia organizada, sobrepasaba los "límites" que exige el respeto del principio de proporcionalidad en relación con los arts. 7,8 y 52.1 de la Carta (par. 69).

Dicho pronunciamiento, referenciado ampliamente por el TJUE en el asunto *Schrems I*, supuso la adopción del denominado *Umbrella Agreement* a través de una nueva Decisión (UE) 2016/920, basada a su vez en una nueva Directiva (UE) 2016/680, ambas relativas al tratamiento de datos personales con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales.

que, aunque el demandante no había cuestionado formalmente su validez, en realidad impugnaba la licitud del régimen de Puerto Seguro establecido en la Decisión 2000/520/CE, planteando dos cuestiones prejudiciales al Tribunal de Justicia al respecto.

De este modo, el asunto *Schrems* (2015) o *Schrems I* constituye el primer pronunciamiento del TJUE en el que se aborda el análisis de las transferencias internacionales de datos de acuerdo con el TUE, el TFUE y la CDFUE, siendo calificado por la doctrina como un pronunciamiento emblemático en defensa del derecho a la protección de datos[20].

En dicho pronunciamiento el TJUE, siguiendo la opinión del Abogado General Y. Bot, concreta por primera vez respecto de las transferencias internacionales de datos personales el concepto de nivel de protección adecuado como fórmula que exige que el tercer país "garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta" (par. 73).

Además, en el asunto *Schrems I* el Tribunal de Justicia aclara que, para considerarse adecuados, los medios articulados en un tercer país para garantizar el nivel de protección no tienen por qué ser idénticos a los utilizados por la Unión Europea, pero sí "deben ser eficaces en la práctica" para garantizar una protección equivalente a la garantizada en la Unión (par. 74) y, como el nivel de protección de un tercer país puede evolucionar compete a la Comisión Europea "comprobar periódicamente" si sigue siendo adecuado el nivel de protección del país en cuestión (par. 76).

El Alto Tribunal de la UE sostiene su fallo en el asunto *Schrems I* sobre dos aspectos esenciales que resultan determinantes para declarar, en última instancia, la invalidez de la Decisión 2000/520/CE.

De un lado, aborda el análisis de la excepción a la aplicación de los principios de Puerto Seguro basada en exigencias de seguridad nacional, interés público y cumplimiento de la ley (estadounidense) prevista en el Anexo I, párrafo cuarto, de la Decisión 2000/520/CE (par. 84). A este respecto, considera que la Decisión de la Unión Europea otorga "primacía" a las exigencias de seguridad nacional, interés público y cumplimiento de la ley norteamericana sobre los principios de Puerto Seguro incorporando, de este modo, una "excepción de carácter general" que posibilita "injerencias" en los derechos

[20] Entre los múltiples comentarios y reflexiones en torno al asunto *Schrems I* a uno y otro lado del Atlántico, pueden consultarse, sin pretensión de exhaustividad, los trabajos de Blanc (2017); Comella (2015); De Miguel Asensio (2015); Kuner (2017); McGinnis y Miller (2015); Puerto y Taibi (2018) y Uría Gavilán (2016).

fundamentales de las personas cuyos datos sean transferidos a EEUU desde la Unión (par. 87)[21].

Recordando las carencias detectadas por la Comisión a las que anteriormente se ha hecho referencia, así como sus argumentos sobre la conservación y acceso por las autoridades públicas con carácter generalizado a los datos personales en el Asunto *Digital Rights Ireland y otros* (2014), el TJUE estima que el art. 1 de la Decisión resultaba inválido en tanto que vulnera las exigencias establecidas en la Directiva 95/46/CE interpretada a la luz de la CDFUE.

De otro lado, el TJUE entra a analizar las capacidades que ostentan las autoridades independientes previstas en el art. 8.3 CDFUE para fiscalizar, a petición de los interesados, el efectivo cumplimiento de los principios de Puerto Seguro. En este sentido concluye que el art. 3 de la Decisión 2000/520/CE "priva a las autoridades nacionales de control" de las facultades que les atribuye la Directiva 95/46/CE interpretada de acuerdo con la CDFUE, sin que el legislador europeo esté habilitado para llevar a cabo dicha restricción sobre la base de una Decisión (pars. 102-103).

Desde tales premisas, el asunto *Schrems I* concluye en el TJUE con la declaración de la invalidez en su conjunto de la Decisión 2000/520/CE y con ella, del sistema de Puerto Seguro (*Safe Harbor*) para la transferencia de datos personales desde la UE a los Estados Unidos. Sin embargo, este aparente vacío normativo que supuso la anulación de la decisión de adecuación en la que se sustentaba el mecanismo del Puerto Seguro, no tardaría en ser colmado por las instituciones europeas y norteamericanas mediante la adopción de una nueva decisión de adecuación que reconociera la licitud de dichas transferencias de datos personales a uno y otro lado del Atlántico.

3. EL NUEVO MARCO DE ADECUACIÓN O EL FUNAMBULISMO JURÍDICO-POLITICO: EL ESCUDO DE PRIVACIDAD (*PRIVACY SHIELD*)

El pronunciamiento del TJUE en 2015 invalidando la decisión de adecuación del Puerto Seguro tuvo como consecuencia la necesidad de las empresas europeas de buscar medios alternativos para llevar a cabo lícitamente las transferencias de datos desde la UE a los EEUU, recurriendo a las cláusulas contractuales tipo o cláusulas tipo (CCT) (*Standard Contractual Clauses*-SCC) y a las normas corporativas vinculantes (NCV) (*Binding Corporate Rules*-BCR).

[21] La interpretación restrictiva de las excepciones al ámbito de aplicación de la Directiva 95/46/CE había sido reconocida por el TJUE en el asunto *František Ryneš* (2014) (par. 29), referenciándola también en el asunto *Puškár* (2017) (par. 38) y en el asunto *Jehovan todistajat* (2018) (par. 37).

En el marco de la Directiva 95/46/CE las cláusulas contractuales tipo se configuraban como un modelo de contrato previamente aprobado por la Comisión Europea para la protección de los datos personales en las transacciones entre empresas ubicadas en terceros Estados[22]. Por su parte, las normas corporativas vinculantes se contemplaban como reglas generales de carácter voluntario adoptadas por grupos multinacionales, siendo sometidas posteriormente a la aprobación del regulador nacional de un Estado miembro de la UE. Su aplicación tenía un carácter global dentro del grupo empresarial, resultando de obligado cumplimiento para todo el grupo con independencia de los países donde radicaran sus sucursales o agencias.

En todo caso, ninguno de estos instrumentos de licitud de las transferencias internacionales podía proporcionar una alternativa de aplicación uniforme al conjunto de las transferencias de datos con origen en todo el territorio UE hacia los EEUU como proporcionaba la decisión de adecuación del Puerto Seguro. Se evidenció pues, la necesidad de "encontrar una solución política" que se tradujera en un nuevo marco jurídico que, respetando los principios establecidos en la Directiva 95/46/CE interpretados a la luz de la CDFUE, proporcionara "mayores garantías" para la transferencia de datos en las relaciones transatlánticas UE-EEUU (Cordero Álvarez, 2019, p. 88).

En esta línea, el 17 de enero de 2014 fue aprobada por las autoridades estadounidenses la Directiva de Política Presidencial 28 (*Presidential Policy Directive 28*- PPD-28) en cuyo marco el Departamento de Seguridad Nacional adoptó el año siguiente la Orden "Protegiendo la información personal recogida de las señales de las actividades de inteligencia" (IA-1002), que impone una serie de restricciones respecto de las actividades de inteligencia de señales, y prevé el nombramiento de un Defensor del Pueblo específico, encargado de la tramitación de las reclamaciones presentadas por ciudadanos de la UE en el ámbito de la protección de datos personales.

Asimismo, la administración estadounidense propuso la adopción de un sistema de recursos jurisdiccionales en los EEUU frente a posibles vulneraciones de los datos personales de los ciudadanos europeos (*Judicial Redress Act, 2015*) a través de la cual, según afirma López Aguilar (2017) "se abre la vía de los *judicial remedies* a ciudadanos no estadounidenses" (p. 563). En efecto, la *Judicial Redress Act* enuncia las condiciones para el otorgamiento

[22] El 15 de junio de 2001 y el 27 de diciembre de 2004 la Comisión Europea adoptó sendas Decisiones en las que se incorporan las cláusulas que regulan la transferencia de datos personales de responsable a responsable del tratamiento a terceros Estados, y mediante la Decisión del 5 de febrero de 2010 estableció las cláusulas tipo de la transferencia de datos personales de responsable a encargado.

Más recientemente, la Decisión de Ejecución (UE) de 2016 (también conocida como Decisión CPT) modifica las adoptadas en 2001 y 2010 en relación a las cláusulas tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países.

de acciones civiles a las que considera "personas protegidas" (*covered person*) en las que deben concurrir simultáneamente los tres requisitos siguientes:

1) El Estado en cuestión, la organización regional de integración económica o un Estado miembro de esta última

— han alcanzado un acuerdo con los Estados Unidos que prevea una protección adecuada de la "*privacy*" para la información compartida con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales; o

— el Fiscal General ha determinado que el Estado en cuestión, la organización regional de integración económica o un Estado miembro de esta última ha compartido "efectivamente" información con los Estados Unidos con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales y protege adecuadamente la información compartida.

2) El Estado en cuestión, la organización regional de integración económica o un Estado miembro de esta última, consiente la transferencia de datos personales con fines comerciales entre su territorio y los Estados Unidos a través de un acuerdo con los Estados Unidos o similar.

3) El Fiscal General certifica que las políticas relativas a la transferencia de datos personales con fines comerciales y las actuaciones del Estado en cuestión, la organización regional de integración económica o un Estado miembro de esta última, no obstaculizan materialmente los intereses de seguridad nacional de los Estados Unidos.

De este modo, la renegociación del sistema Puerto Seguro acordado entre la UE y los EEUU se tradujo en el nacimiento de un nuevo instrumento de adecuación para la transferencia de datos personales transatlántica denominado Escudo de Privacidad (*Privacy Shield*), teniendo presente, como demuestra la referencia explícita en los Considerandos 9 a 11 de la Decisión de Ejecución (UE) 2016/1250 (Decisión EP), lo declarado por el TJUE en el asunto *Schrems I*.

Sin embargo, como se comprobará a continuación, más allá de una formulación más detallada de los principios de la transferencia de datos, el Escudo de Privacidad no incorpora grandes novedades respecto a las garantías aplicables a la transferencia de datos personales UE-EEUU en el marco del Puerto Seguro, siendo calificado como una "suave actualización" de su predecesor (Gonzalo Domenech, 2019, p. 366).

El nuevo instrumento de adecuación de la transferencia de datos personales acordado entre la UE y los EEUU mediante la Decisión de Ejecución (UE) 2016/1250 entró en vigor el 1 de agosto de 2016, y fue objeto de análisis por el Grupo de Trabajo del Artículo 29 (GT 29) a través de dos documentos fechados ambos el 13 de abril de 2016.

De un lado, el Documento de trabajo (WP 237, 2016) relativo a las garantías europeas esenciales en la transferencia de datos personales y, de otro, el Documento sobre el acuerdo EU-EEUU relativo al Escudo de Privacidad (WP

238, 2016) elaborado desde la perspectiva de la inminente aprobación del Reglamento (UE) 2016/679, General de Protección de Datos (RGPD) que estaba a punto de adoptarse -el 27 de abril de 2016- por las instituciones europeas.

En su Documento sobre el acuerdo del Escudo de Privacidad (WP 238) el Grupo de Trabajo admitía, con carácter general, las mejoras que incorporaba este nuevo marco jurídico de las transferencias de datos personales entre la UE y los EEUU con respecto al fallido sistema de Puerto Seguro (WP 238, 2016, p. 2). También valoraba positivamente la adopción de la *Judicial Redress Act* por los EEUU, aunque mostraba su escepticismo acerca de la efectividad de su aplicación a los ciudadanos europeos (WP 238, 2016, p. 35).

Esta última duda era compartida por el Supervisor Europeo de Protección de Datos (*European Data Protection Supervis*or-EDPS por sus siglas en inglés), en su Informe relativo al borrador de acuerdo UE-EEUU sobre el Escudo de Privacidad. En su opinión, la normativa estadounidense únicamente se aplicaba a los datos transferidos "directamente" desde entidades públicas o privadas de los países denominados "cubiertos" —como los Estados miembros de la UE— a las autoridades públicas norteamericanas, pero excluía los datos personales transferidos entre "entidades privadas" a través del Escudo de Privacidad a los que pueden tener acceso las autoridades de los EEUU (EDPS, 2016, p.11).

En todo caso, uno de los aspectos en los que hacía especial hincapié el Documento WP 238 del Grupo de Trabajo del Art. 29 es la regulación de las excepciones por motivos de seguridad nacional y el acceso a los datos personales por parte de las autoridades públicas, tanto europeas como estadounidenses. En relación a tales aspectos se remite al WP 237, donde se enuncian las "garantías europeas esenciales" (*European Essential Guarantees*) que permiten justificar las injerencias en los derechos a la vida privada y a la protección de datos (arts. 7 y 8 CDFUE) cuando se lleven a cabo transferencias de datos personales.

En concreto, en el WP 237 del Grupo de Trabajo se afirmaba que el procesamiento de los datos personales ha de basarse en normas claras, precisas y accesibles; que deben acreditarse la necesidad y la proporcionalidad respecto de los objetivos perseguidos; que las garantías efectivas deben ser accesibles para los interesados, y que resulta exigible la existencia de un mecanismo de supervisión independiente (WP 237, 2016, p. 6).

Acerca de la existencia de mecanismos de supervisión independientes, el Grupo de Trabajo estimaba que "la representación de la Oficina del Director de Inteligencia Nacional (ODNI) no excluye la recogida masiva e indiscriminada de datos personales provenientes de la UE", recordando su consideración de que el respeto de los derechos fundamentales exige que estas actividades deban ser valoradas como proporcionadas y estrictamente necesarias en una sociedad democrática (WP 238, 2016, p. 4).

Más aún, en opinión del Supervisor Europeo de Protección de Datos en su Dictamen de 30 de mayo de 2016, el proyecto de acuerdo del Escudo de

Privacidad "no evalúa adecuadamente las posibilidades de que los interesados ejerciten sus derechos de acceso, rectificación o cancelación" respecto de los datos "recogidos o accesibles por autoridades públicas con fines distintos de la seguridad nacional", como por ejemplo en cumplimiento de la "ley nacional" o de fines de "interés público". Pero también pone de manifiesto sus dudas sobre el *Privacy Shield* cuando recuerda que cualquier regulación que se proponga un mínimo de estabilidad en su aplicación "debería tomar en consideración el nuevo marco europeo de protección de datos" –en clara referencia al Reglamento (UE) General de Protección de Datos (RGPD), aprobado el 27 de abril de ese mismo año[23]-.

A juicio del Supervisor Europeo de Protección de Datos, el nuevo RGPD resulta "esencial para proporcionar un nivel adecuado de protección y seguridad jurídica" con respecto a los principios básicos de la protección de datos personales en la UE, subrayando la circunstancia de que incorpora nuevos elementos que no estaban presentes en la Directiva 95/46 (EDPS, 2016, pp. 11-12).

A pesar de los reparos que se aprecian en los análisis emitidos por el Grupo de Trabajo del Art. 29 y por el Supervisor Europeo de Protección de Datos con respecto a la adopción del sistema del Escudo de Privacidad cuyo funcionamiento se basa, nuevamente, en la autocertificación de las entidades norteamericanas, la Decisión de Ejecución 2016/1250 fue aprobada por la Comisión Europea con arreglo a la Directiva 95/46/CE.

La simple lectura de los Considerandos 10 y 11 de esta nueva Decisión de Ejecución pone de relieve cierto espíritu crítico por parte de la Comisión Europea, respecto de las insuficiencias que conllevaron la declaración de invalidez del sistema de Puerto Seguro por el Tribunal de Justicia en el asunto *Schrems I*. Sin embargo, el Considerando 13 de la Decisión de Ejecución subraya que en relación con el acuerdo relativo al Escudo de Privacidad la propia Comisión "ha analizado con detenimiento el Derecho y las prácticas vigentes en los Estados Unidos", alcanzando la conclusión de que "garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión a entidades autocertificadas establecidas en los Estados Unidos"[24].

---

[23] En efecto, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo fue adoptado el 27 de abril de 2016 pero, como resulta conocido, su art. 99.2 difiere su aplicabilidad al 25 de mayo de 2018 aunque el apartado 1 del mismo precepto lo declara vigente transcurridos veinte días desde su publicación en el *Diario Oficial de la Unión Europea*, circunstancia que tuvo lugar el 4 de mayo de 2016.

[24] La Decisión de Ejecución 2016/1250 de la Comisión Europea (Decisión EP) consta de 155 Considerandos pero únicamente de 6 artículos, incluyendo en su publicación en el Diario Oficial un desmesurado número de Anexos y Apéndices (pp. 37 a 112) entre cuyos contenidos se encuentran una Carta de la Secretaria de Comercio Estadounidense (Sra. P. Pritzker); una Carta del Subsecretario de Comercio Internacional en funciones (Sr. K. Hyatt); una Carta de la Presidenta de la Comisión Federal de Comercio (Sra. E. Ramirez); una Carta del Secretario de Transporte estadounidense (Sr. A. Foxx); una Carta del Secretario de Estado estadounidense (Sr. J. Kerry),

Pero las dudas acerca de la efectividad de las garantías que el *Privacy Shield* proporcionaba a la transferencia de datos personales entre la UE y los EEUU también se aprecian en el primer Informe de revisión realizado por la Comisión Europea en 2017. Un Informe que concluye reiterando la apreciación de que los Estados Unidos continúan proporcionando un adecuado nivel de protección a las transferencias de datos provenientes de la UE en el marco del Escudo de Privacidad pero que, al mismo tiempo, formula diez recomendaciones para mejorar su funcionamiento práctico (COM, 2017b, pp. 4-7)[25].

Menos ambiguo resultó el Documento adoptado por Grupo de Trabajo del Art. 29 (WP 255) cuando al evaluar el primer año de vigencia del Escudo de Privacidad en 2017, afirmaba haber encontrado significativos aspectos que necesitaban ser puestos en conocimiento de la Comisión Europea y de las autoridades norteamericanas con el fin de adoptar acciones inmediatas al respecto.

En concreto, estimaba necesario priorizar la designación de un Defensor del Pueblo "independiente", al tiempo que instaba a explicar "más detalladamente" las reglas procedimentales, incluida la desclasificación. Unas indicaciones que no quedaban en meras sugerencias en tanto que el Grupo de Trabajo amenazaba con someter a juicio de las jurisdicciones nacionales la decisión de adecuación del *Privacy Shield*, para que estas presentaran una cuestión prejudicial al TJUE si no se resolvían las cuestiones indicadas (WP 255, 2017, p. 20).

Por su parte, la Resolución del Parlamento Europeo de 5 de julio de 2018 (PE, 2018a) manifestaba su preocupación por el hecho de que en el marco de la legislación presupuestaria general aprobada en marzo de ese mismo año, el Congreso de los EEUU hubiera promulgado la Ley de aclaración de la utilización de datos extranjeros [*Clarifying Lawful Overseas Use of Data Act - Cloud Act* (H.R. 4943)]. Una legislación, que según afirma, "facilita el acceso policial" al contenido de comunicaciones y otros datos relacionados, incluso cuando estén almacenados fuera del territorio estadounidense.

Además, el Parlamento Europeo también expresaba su desconfianza respecto de la firma de "acuerdos ejecutivos" de terceros Estados con los Estados Unidos para "autorizar a los proveedores de servicios estadounidenses a responder a ciertas órdenes extranjeras para acceder a datos de comunicaciones" (PE, 2018a, par. Q).

De este modo, podría entenderse junto a Cordero Álvarez (2019) y Syed & Yilmaz Genç (2019), que la aprobación de la *Cloud Act* incrementaba la incertidumbre sobre la licitud de las transferencias de datos personales entre la UE y los EEUU.

---

y una Carta del Asesor General (Sr. R. Litt) de la Oficina del Director de Inteligencia Nacional de los EEUU.

[25] La primera revisión anual del funcionamiento del *Privacy Shield* tuvo lugar en septiembre de 2017 en Washington, DC, y el 18 de octubre de ese mismo año la Comisión remitió su Informe al Parlamento Europeo y al Consejo [COM(2017) 611 final].

Una apreciación a la que conviene añadir la constatación de un conjunto de deficiencias "persistentes" que el Parlamento Europeo observa en el Escudo de Privacidad y que afectan a la garantía de los derechos fundamentales (PE, 2018a, par. 1)[26]. Entre ellas, se enumeraban la existencia de declaraciones falsas de certificación; la complejidad para los ciudadanos europeos de los procedimientos de recurso; los usos indebidos de datos personales revelados por Facebook y Cambridge Analytica[27] y, en última instancia, la constatación de que el Escudo de privacidad no sigue el modelo de la UE basado en el consentimiento y en la previsión de excepciones muy limitadas a los derechos de cancelación y oposición (PE, 2018a, pars. 10-14,18).

Más contundentemente, el Parlamento Europeo "deplora" que las autoridades estadounidenses y la Comisión Europea no hayan iniciado las conversaciones dirigidas a dar cumplimiento a las recomendaciones formuladas por el Grupo de trabajo del Art. 29 concluyendo que, en las condiciones vigentes en ese momento, el Escudo de Privacidad "no proporciona el nivel adecuado de protección" exigido por el Tribunal de Justicia (PE, 2018a, pars. 32, 34).

En opinión del Parlamento Europeo, a menos que los EEUU cumplieran plenamente las condiciones citadas antes del 1 de septiembre de ese mismo año, la Comisión habría dejado de actuar bajo la cobertura del Reglamento General de Protección de Datos (RGPD). A tales efectos, proponía la suspensión de la aplicación del Escudo de Privacidad hasta que tuviera lugar dicho cumplimiento por las autoridades estadounidenses, y encargaba a su Comisión de Libertades Civiles, Justicia y Asuntos de Interior el control sobre el acuerdo del Escudo de Privacidad, incluidos los recursos presentados ante el

---

[26] Comentando la *Cloud Act, vid*., por todos, Meyer (2018).

De hecho, la aprobación de la Cloud Act viene a sumarse a la adopción del Decreto de mejora de la salud pública en los EEUU (*Executive Order 13768, Enhancing Public Safety in the Interior of the United States*), en virtud del cual se penaliza en la percepción de fondos federales a las ciudades que rechacen la aplicación de la legislación de inmigración —denominadas *"sanctuary cities"*—. Entre las sanciones previstas se incluye la no aplicación de la legislación norteamericana sobre protección de datos a personas extranjeras.

Asimismo, las Cámaras derogaron la protección de la privacidad acordada en diciembre de 2016 para los clientes de banda ancha y otros servicios de telecomunicaciones (*rule submitted by the Federal Communications Commission relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services'*).

[27] El escándalo que vinculó a Cambridge Analytica (Reino Unido) y Facebook (EEUU) que supuso el uso por la empresa británica de los datos de los perfiles de la red social estadounidense para generar anuncios personalizados con fines políticos, dio lugar a la Resolución del Parlamento Europeo de 25 de octubre de 2018 (PE, 2018b), en la que solicitaba a los organismos de la UE la realización de una auditoría completa de Facebook para evaluar el grado de protección de los datos personales de sus usuarios. Además, para evitar la manipulación electoral a través de ellos proponía una serie de medidas, reconociendo la gravedad de un asunto que afecta a la solidez de los sistemas democráticos en todo el mundo.

TJUE pendientes de resolución[28], así como la realización de un seguimiento del grado de cumplimiento de las recomendaciones formuladas (PE, 2018a, pars. 35-36).

Ante los graves "problemas de eficacia y alcance que este nuevo marco" había manifestado desde su puesta en práctica, y pese a que algunas de las medidas recomendadas por la Comisión Europea fueron implementadas por las autoridades estadounidenses, el Parlamento Europeo no confiaba en la duración del Escudo de Privacidad (Cordero Álvarez, 2019, p. 93).

Por su parte, el Informe de la Comisión sobre la segunda revisión anual del funcionamiento del *Privacy Shield* efectuada en octubre de 2018 en Bruselas (COM (2018) 860 final), instaba a las autoridades norteamericanas a diseñar un marco general de regulación de la privacidad y de la protección de datos, animándole a adherirse al Protocolo 108 del Consejo de Europa (COM, 2018, pp. 5-6).

La aplicación general del RGPD en el conjunto de los Estados integrantes del EEE proporcionó a la Comisión, nuevamente, la oportunidad de defender la conformidad con las garantías europeas del *Privacy Shield*. Así, en el balance sobre su impacto respecto de las transferencias internacionales de datos realizado en su Comunicación de 24 de julio de 2019 (COM(2019) 374 final), destaca la utilidad del Escudo de Privacidad para "garantizar los flujos de datos transatlánticos sobre la base de un nivel elevado de protección" (COM, 2019a, p. 13).

La Comunicación relativa a la tercera revisión del Escudo de Privacidad UE-EEUU [COM(2019) 495 final], reconoce que se han analizado tanto aspectos comerciales como cuestiones relativas al acceso de las autoridades públicas de los EEUU a los datos personales. En relación con este último aspecto, la Comisión acoge las aclaraciones de las autoridades norteamericanas sobre el funcionamiento de los programas *PRISM* y *UPSTREAM*, incluida la afirmación de que dichos programas no se aplican a las recopilaciones indiscriminadas de datos como las que llevan a cabo empresas certificadas con respecto al tratamiento de datos transferidos desde la UE al amparo del Escudo de Privacidad (COM, 2019b, p. 6).

En todo caso, la tercera revisión anual del Escudo de Privacidad realizada en Washington DC vino marcada por la proximidad temporal de la resolución por el TJUE en el conocido como asunto *Schrems II*, que podía conllevar la posible anulación de la Decisión de Ejecución 2016/1250 en la que se fundamentaba el Escudo de Privacidad. En efecto, como se verá en las páginas que siguen, el Alto Tribunal de la UE todavía no había dicho la última palabra

[28] Entre ellos, el recurso interpuesto el 25 de octubre de 2016 por *La Quadrature du Net y otros v. Comisión* (Asunto T-738/16), en el que se solicitaba que se declarase que la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, sobre la que se sustenta el acuerdo del *Privacy Shield* era contraria a los arts. 7, 8 y 47 de la CDFUE y, en consecuencia, fuera invalidada.

acerca de las transferencias de datos personales UE-EEUU sustentadas en el Escudo de Privacidad.

4. LA SENTENCIA *SCHREMS II* Y LA INVALIDEZ DEL ESCUDO DE PRIVACIDAD (*PRIVACY SHIELD*)

Tras la declaración de invalidez por TJUE de la Decisión 2000/520 en el asunto *Schrems I*, las actuaciones procesales se retrotrajeron al momento de la reclamación del Sr. Schrems ante la autoridad irlandesa de protección de datos. Su investigación puso de manifiesto que gran parte de los datos personales alojados en Facebook Ireland se transferían a Facebook Inc. (EEUU) a través de cláusulas tipo de protección de datos basadas en la Decisión de Ejecución 2010/87/UE (Decisión CPT) pero contenidas en uno de los Anexos de la Decisión de Ejecución 2016/1250 (Decisión EP) que constituye la decisión de adecuación en la que se fundamenta el Escudo de Privacidad UE-EEUU.

A instancia de la autoridad de protección de datos, el Sr. Schrems modificó su reclamación alegando que el Derecho estadounidense impone a Facebook Inc., la obligación de poner los datos personales que se transfieren desde la UE a disposición de autoridades estadounidenses como la National Security Agency (NSA) y la Federal Bureau of Investigation (FBI), donde son utilizados en el marco de programas de vigilancia de las autoridades gubernamentales norteamericanas vulnerando los arts. 7, 8 y 47 de la CDFUE. En tales circunstancias, a juicio del Sr. Schrems, la Decisión de Ejecución 2016/1250 (Decisión EP) no puede proporcionar cobertura lícita a la transferencia internacional de esos datos, por lo que solicita el cese inmediato de la transferencia de sus datos personales a Facebook Inc.[29]

En puridad, la pretensión del Sr. Schrems únicamente cuestiona de modo directo la validez de las cláusulas tipo adoptadas por la Comisión mediante la Decisión 2010/87/UE (Decisión CPT) por contravenir los arts. 7, 8 y 47 de

[29] La batalla legal del Sr. Schrems contra Facebook se ha trasladado también a los órganos jurisdiccionales austríacos donde interpuso una demanda contra Facebook Ireland Ltd., por no haberle facilitado todos los datos recopilados por la compañía sobre él, además de haber modificado la redacción de los términos de uso y cláusulas contractuales generales como consecuencia de la aplicación efectiva del RGPD.

En la reciente Sentencia de 28 de diciembre de 2020, el Tribunal Superior Regional de Viena condena a Facebook Ireland Limited a pagar al Sr. Schrems 500 euros en concepto de daños emocionales y a concederle pleno acceso a todos los datos que Facebook posea sobre él (asunto *Maximilan Schrems v. Facebook Ireland Limited*, 2020, pars. 2.3.1 y 2.3.2). Al mismo tiempo, el tribunal regional vienés estima que Facebook no necesita obtener de nuevo el consentimiento de todos los usuarios para utilizar sus datos en aplicación del art. 6.1.a) RGPD, sino que puede autoatribuirse el derecho a utilizarlos en sus términos y condiciones en virtud del art. 6.1.b) RGPD, es decir, considerando que el tratamiento de los datos forma parte de la ejecución de un contrato con el interesado (*Ut supra*, par. 3.1.3).

la Carta pero, en última instancia, pone en entredicho la validez de la Decisión de adecuación 2016/1250 del Escudo de Privacidad UE-EEUU (Decisión EP), al suscitar la duda acerca del nivel de protección adecuado constatado por la Comisión respecto de las injerencias de los servicios de inteligencia estadounidenses respecto de los derechos fundamentales de los ciudadanos europeos cuyos datos personales son transferidos a este tercer país.

De este modo, apoyándose en la legitimación activa para promover un procedimiento jurisdiccional que la Sentencia del TJUE *Schrems I* reconoce a las autoridades nacionales de protección de datos (par. 65), la autoridad irlandesa de protección de datos inició un procedimiento ante la High Court de Irlanda (Tribunal Superior) con el fin de que este planteara una cuestión prejudicial al Tribunal de Justicia en la que se dilucidara esta cuestión.

Mediante resolución de 4 de mayo de 2018 el Tribunal Superior de Irlanda plantea el reenvío prejudicial al TJUE, formulando once cuestiones prejudiciales que serán resueltas mediante la Sentencia de 16 de julio de 2020 (asunto *Schrems II*), que constituye el primer pronunciamiento del Alto Tribunal de la UE en el que analiza las garantías adecuadas para las transferencias internacionales de datos personales una vez derogada la Directiva 95/46/CE.

4.1. La aplicación del RGPD a las transferencias de datos personales objeto de tratamiento con fines de seguridad nacional

En la primera cuestión prejudicial, la High Court de Irlanda plantea al TJUE la dilucidación de si una transferencia de datos personales realizada por un operador económico establecido en un Estado miembro a otro operador económico establecido en un tercer país está comprendida en el ámbito de aplicación del RGPD, cuando en el transcurso de esa transferencia o con posterioridad a ella, esos datos pueden ser objeto de tratamiento por las autoridades del tercer país con fines de seguridad nacional, defensa y seguridad del Estado.

En relación con esta cuestión, el Tribunal Superior irlandés remite al TJUE su propia Sentencia de 3 de octubre de 2017(asunto *The Data Protection Commissioner & Facebook Ireland & Maximillian Schrems*), en la que había apreciado que las autoridades de inteligencia norteamericanas tienen acceso a los datos y a la vigilancia de personas no nacionales de los EEUU que se encuentren fuera del territorio de ese país.

El Tribunal Superior de Irlanda asume en su pronunciamiento el argumento planteado por la autoridad irlandesa de protección de datos según el cual, las cláusulas tipo aplicables al exportador y al importador de datos no resultan vinculantes para las autoridades del tercer país quienes pueden exigir al importador de datos que facilite, con fines de seguridad nacional, los datos personales que le han sido transferidos (High Court, 2017, pars. 40-41).

Después de analizar detalladamente el funcionamiento de los distintos programas articulados por las agencias de seguridad nacional estadounidenses con respecto a los datos que circulan a través de internet, el Tribunal Superior irlandés alcanza la conclusión de que los EEUU llevan a cabo un tratamiento de datos en masa sin las garantías de una protección equivalente a la que proporcionan los arts. 7 y 8 de la CDFUE.

A su juicio, resulta probado que las empresas de telecomunicaciones que explotan la "red troncal" de internet están obligadas a permitir a la NSA la copia y el filtro de las comunicaciones enviadas o recibidas por el nacional no americano que se corresponda con un "selector", accediendo de este modo a los metadatos y al contenido de las comunicaciones de que se trate, así como a los datos "en tránsito" hacia los EEUU a través de los cables situados en el lecho marino del Atlántico (High Court, 2017, pars. 164-193).

Del mismo modo, tras un exhaustivo análisis de los procedimientos jurisdiccionales de tutela de los derechos a la vida privada y familiar, y a la protección de datos de carácter personal (arts. 7 y 8 CDFUE), el Tribunal irlandés alcanza la conclusión de que los ciudadanos de la UE no tienen acceso a los mismos recursos jurisdiccionales ni en las mismas condiciones que los nacionales estadounidenses. En primer término, porque la Cuarta Enmienda de la Constitución de los Estados Unidos que constituye la norma más importante en el ordenamiento jurídico norteamericano de protección contra la vigilancia ilegal, no resulta aplicable a los ciudadanos de la UE. En segundo lugar, en tanto que la figura del Ombudsman que prevé el Escudo de Privacidad no constituye un órgano jurisdiccional en el sentido del art. 47 CDFUE (High Court, 2017, pars. 251-263).

En su pronunciamiento acerca de esta cuestión en el asunto *Schrems II*, el TJUE comienza por recordar su jurisprudencia acerca del carácter restrictivo con el que deben ser interpretadas las excepciones a la aplicación de la normativa europea de protección de datos.

En su opinión, la excepción a la aplicación del RGPD prevista en su art. 2.2, letra c) se refiere al supuesto del tratamiento de datos efectuado por una persona física para uso exclusivamente personal o doméstico (par. 85), y las excepciones contempladas en el art. 2.2, letras a), b) y d), enuncian supuestos de actividades estatales o de autoridades estatales, pero en todo caso, ajenas a las actividades de los particulares sean estos personas físicas o jurídicas.

Como punto de partida, el TJUE considera que el RGPD no puede ser excluido de la aplicación a las transferencias internacionales de datos personales entre "dos operadores económicos con fines comerciales" como es el caso de Facebook Ireland y Facebook Inc., cuando "en el transcurso de la transferencia o tras ella" los datos personales puedan ser objeto de un tratamiento "con fines de seguridad pública, defensa o seguridad del Estado por parte de las autoridades del país tercero de que se trate" (par. 86).

Resultando aplicable el RGPD a las transferencias de datos en tales circunstancias, el Alto Tribunal de la UE analiza la legitimidad de la injerencia que supone el tratamiento con fines de seguridad nacional por las autoridades públicas norteamericanas de los datos personales transferidos a los EEUU con fines comerciales desde la perspectiva de la existencia de un control jurisdiccional "efectivo" que según el art. 47 CDFUE, garantice el cumplimiento en el tercer país de las disposiciones del Derecho de la Unión (par. 187), entendiendo que el art. 47 CDFUE implica la existencia de "posibilidades efectivas de acciones administrativas y judiciales".

De hecho, la vigencia del derecho a la tutela judicial efectiva y a un juez imparcial (art. 47 CDFUE) constituyen elementos que deben ser tomados en consideración por la Comisión según el art. 45.2 RGPD, para adoptar la decisión de adecuación que constata la concurrencia en el tercer país de un grado de protección sustancialmente equivalente al garantizado en la Unión por el RGPD.

Sin embargo, el reconocimiento por la Comisión de la existencia de un control jurisdiccional acorde con el art. 47 CDFUE que proporciona a los ciudadanos europeos una tutela eficaz ante reclamaciones basadas en un tratamiento de datos personales supuestamente ilegal en el país tercero, únicamente toma en consideración la existencia del Defensor del Pueblo creado en el ámbito del Escudo de Privacidad en los EEUU. Una institución que, según estima el TJUE en el asunto *Schrems II*, "no puede subsanar las lagunas" constatadas por la propia Comisión en la Decisión 2016/1250 (Decisión EP) cuando admite la "inexistencia de vías de recurso" frente a injerencias de las autoridades públicas norteamericanas a través de distintos programas de vigilancia con fines de seguridad nacional.

Por este motivo, el Alto Tribunal de la UE entiende en el asunto *Schrems II* que la Comisión no pudo concluir válidamente de acuerdo con el art. 45 RGPD, que los EEUU garantizaban un nivel de protección sustancialmente equivalente respecto del art. 47 CDFUE (pars. 190-191).

Aun cuando pudiera parecer que la cuestión quedaba zanjada con los argumentos anteriormente expuestos en los que se concluye que el Defensor del Pueblo no puede suplir la ausencia de acciones en Derecho ejercitables por los ciudadanos europeos en los EEUU ante un tribunal independiente e imparcial para la tutela de sus datos personales, el Tribunal de Justicia vuelve a examinar la figura del Defensor del Pueblo para analizar si los requisitos de su designación y la atribución de sus competencias, posibilitan la subsanación de la quiebra constatada anteriormente respecto del art. 47 CDFUE.

Tampoco desde esta perspectiva es posible para el TJUE considerar que la figura del Defensor del Pueblo puede garantizar un nivel sustancialmente equivalente de protección jurisdiccional de los datos personales como el exigido en el art. 47 CDFUE, en tanto que dicha institución no se configura en el ordenamiento jurídico norteamericano con las necesarias garantías de independencia respecto del Poder ejecutivo, ni tiene asignadas facultades que

le permitan adoptar decisiones vinculantes para el servicio de inteligencia de los EEUU (pars. 195-196).

4.2. Decisiones de adecuación *vs*. cláusulas tipo de protección de datos

El análisis del TJUE contraponiendo las garantías adecuadas que ofrecen las decisiones de adecuación a las proporcionadas por las cláusulas tipo de protección de datos resulta la argumentación de mayor peso en la *ratio decidendi* del asunto *Schrems II*, pudiendo diferenciarse en torno a ella dos aspectos. De un lado, el reconocimiento de distintas facultades a las autoridades de control independientes para valorar el nivel de protección adecuado ofrecido por el tercer país atendiendo al instrumento de licitud en el que se basa la transferencia internacional de datos personales. De otro lado, la afirmación de que no existen diferencias entre ambos mecanismos de transferencia internacional de datos personales en cuanto a la exigencia de cumplimiento de las garantías adecuadas según los elementos enunciados en el art. 45.2 RGPD aun cuando el TJUE formule al respecto argumentos contradictorios que terminan por diferenciar en este aspecto a las decisiones de adecuación y las cláusulas contractuales tipo.

4.2.1. Distintas facultades de las autoridades de control independientes atendiendo al instrumento de licitud

Al abordar el tratamiento de las competencias de las autoridades de control independientes respecto de las transferencias internacionales de datos personales, el TJUE reconoce la existencia de diferencias dependiendo de si la transferencia de datos personales a un tercer país tiene como fundamento de licitud la adopción de una decisión de adecuación o la aplicación de cláusulas tipo de protección de datos.

Remitiéndose a la Sentencia *Schrems I*, el TJUE recuerda que las autoridades de control competentes están sujetas al cumplimiento de la Decisión adoptada por la Comisión en el marco del art. 45. 1, frase primera RGPD, en la que esta institución de la Unión constata que un tercer país garantiza un nivel de protección adecuado, sin que las transferencias de datos personales amparadas en una decisión de adecuación requieran de "ninguna autorización específica" (par. 116). Así lo reconoce, por lo demás, el Considerando 103 RGPD al afirmar que

> La Comisión puede decidir, con efectos para toda la Unión, que un tercer país, un territorio o un sector específico de un tercer país, o una organización internacional ofrece un nivel de protección de datos adecuado, aportando de esta forma en toda la Unión seguridad y uniformidad jurídicas en lo que se refiere al tercer país u organización internacional que se considera ofrece tal nivel de

> protección. En estos casos, se pueden realizar transferencias de datos personales a estos países sin que se requiera obtener otro tipo de autorización.

El TJUE pone en relación dicho Considerando del RGPD con el Derecho originario recordando que atendiendo al art. 288 TFUE las decisiones son obligatorias en todos sus elementos y respecto de todos los Estados miembros, salvo que designe destinatarios específicos.

De este modo, el carácter vinculante de las decisiones de adecuación cuando constatan, atendiendo al RGPD que un tercer país garantiza el nivel de protección adecuado y autorizan las transferencias internacionales de datos personales que tengan a este tercer país como destinatario, alcanza a todos los órganos de los Estados miembros, incluidas las autoridades nacionales de protección de datos. En consecuencia, según afirma el Alto Tribunal de la UE, mientras la decisión de adecuación del Escudo de Privacidad (Decisión 2016/1250-Decisión EP) no haya sido declarada inválida por el TJUE, los Estados miembros y sus órganos "no pueden […] adoptar medidas contrarias" a la misma como sería el caso de una apreciación con efecto obligatorio de que el tercer país en cuestión no garantiza el nivel de protección adecuado (pars. 117-118).

En principio, pues, las autoridades nacionales de protección de datos no pueden adoptar medidas que cuestionen una decisión de adecuación. Sin embargo, la decisión de adecuación adoptada en virtud del art. 45.2 RGPD no puede impedir a las personas cuyos datos son objeto de transferencia a un tercer país la posibilidad de presentar reclamaciones ante la autoridad nacional de control (art. 77 RGPD), ni puede tener como consecuencia limitar o anular las facultades reconocidas a las autoridades nacionales de control respecto de las normas reguladoras de la protección de datos.

De ahí que el Alto Tribunal de la UE considere, siguiendo su criterio en el asunto *Schrems I*, que a pesar de existir una decisión de adecuación adoptada por la Comisión, la autoridad nacional de control puede tramitar las reclamaciones de los particulares dirigidas a proteger los derechos y libertades frente al tratamiento de datos personales, disponiendo de capacidad para apreciar "con toda independencia" si la transferencia de estos datos cumple las exigencias establecidas en el RGPD y, en su caso, "interponer un recurso ante los tribunales nacionales" para que estos, si lo estiman procedente, planteen el reenvío prejudicial sobre la validez (pars. 119-120).

Por el contrario, cuando la transferencia de datos personales a un tercer país no tenga su fundamento en una decisión de adecuación como es el caso de las cláusulas contractuales tipo, las autoridades nacionales de control, en virtud del art. 4 de la Decisión de Ejecución 2010/87/UE (Decisión CPT) tienen reconocida por sí mismas, la facultad "prohibir o suspender una transferencia de datos personales" cuando verifiquen que se está realizando "en infracción del Derecho de la Unión o de la legislación nacional en materia de protección de datos" (pars. 115 y 121).

4.2.2. ¿Distinto instrumento de licitud, pero idénticas garantías?

A través de las cuestiones prejudiciales segunda, tercera y sexta, el Tribunal Superior irlandés plantea al TJUE la clarificación acerca del nivel de protección exigido por el art. 46.1 y 2, letra c) RGPD, a las transferencias internacionales de datos personales a un tercer país basadas en cláusulas tipo de protección de datos adoptadas por la Comisión como la Decisión de Ejecución 2010/87/UE (Decisión CPT).

Aunque el Alto Tribunal de la UE reconoce que el art. 46 RGPD "no precisa la naturaleza" de los requisitos derivados de las expresiones "garantías adecuadas", "derechos exigibles", y "acciones legales efectivas", entiende que la interpretación sistemática del RGPD permite considerar que dicha norma pretende establecer un nivel de protección que debe garantizarse con independencia de cuál sea el instrumento de licitud utilizado para llevar a cabo la transferencia de datos personales a un tercer país (par. 92).

De este modo, siguiendo la opinión expresada en las Conclusiones del Abogado General Sr. Henrik Saugmandsgaard Øe, el TJUE considera que las garantías adecuadas a los efectos del art. 45, apartado 1, primera frase RGPD, tanto en las transferencias de datos realizadas mediante cláusulas tipo como a través de decisiones de adecuación deben asegurar que las personas cuyos datos personales se transfieren a un país tercero gozan "de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión" (par. 96).

Por ello, las transferencias internacionales de datos basadas en el art. 46.2.c) RGPD, es decir, a través de cláusulas tipo de protección de datos adoptadas por la Comisión requieren una evaluación que tome en consideración tanto las "estipulaciones contractuales" adoptadas entre el responsable o el encargado del tratamiento establecidos en la Unión y el destinatario de la transferencia establecido en el país tercero, como la regulación jurídica de ese tercer país respecto del eventual acceso de las autoridades públicas a los datos personales transferidos, en los términos a los que se remite el art. 45.2 RGPD (par. 104).

En consecuencia, el TJUE considera que la comprobación de la regulación jurídica en el tercer país atendiendo a los elementos enunciados en el art. 45.2 RGPD resulta exigible para constatar la concurrencia de las garantías adecuadas en las transferencias internacionales de datos, tanto cuando se adopta una decisión de adecuación como cuando se verifican las transferencias sustentadas en cláusulas contractuales tipo de protección de datos adoptadas por la Comisión.

Concretamente el Alto Tribunal de la UE afirma, respondiendo a las cuestiones prejudiciales segunda, tercera y sexta, que

> "el artículo 46, apartados 1 y 2, letra c), del RGPD debe interpretarse en el sentido de que las garantías adecuadas, los derechos exigibles y las acciones legales efectivas requeridas por dichas disposiciones deben garantizar que los derechos de las personas cuyos datos personales se transfieren a un país tercero sobre la

> base de cláusulas tipo de protección de datos gozan de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión por el referido Reglamento, interpretado a la luz de la Carta. A tal efecto, la evaluación del nivel de protección garantizado en el contexto de una transferencia de esas características debe, en particular, tomar en consideración tanto las estipulaciones contractuales acordadas entre el responsable o el encargado del tratamiento establecidos en la Unión y el destinatario de la transferencia establecido en el país tercero de que se trate como, por lo que atañe a un eventual acceso de las autoridades públicas de ese país tercero a los datos personales de ese modo transferidos, los elementos pertinentes del sistema jurídico de dicho país y, en particular, los mencionados en el artículo 45, apartado 2, del referido Reglamento" (par. 105)

Sin embargo, al resolver las cuestiones prejudiciales séptima y undécima planteadas por la High Court irlandesa, el Alto Tribunal de la Unión analiza la Decisión de la Comisión 2010/87/UE (Decisión CPT) donde se contienen las cláusulas contractuales tipo de protección de datos adoptadas por la Comisión, utilizando un criterio reduccionista respecto de los aspectos que se deben valorar para determinar la existencia de un nivel adecuado de protección.

En efecto, afirmando que, a diferencia de las decisiones de adecuación, el carácter contractual de las cláusulas tipo de protección de datos adoptadas mediante una Decisión de la Comisión en aplicación del art. 46.2, c) RGPD no resultan vinculantes para las autoridades públicas de países terceros (par. 125), el TJUE entiende justificado que se obvie la toma en consideración de los elementos enunciados en el art. 45.2 RGPD y se valoren exclusivamente las "estipulaciones contractuales" adoptadas entre el responsable o el encargado del tratamiento establecidos en la Unión y el destinatario de la transferencia establecido en el tercer país a efectos de determinar si concurre las garantías adecuadas de protección de datos.

De este modo, el TJUE termina introduciendo una diferencia sustantiva respecto de los requisitos a tomar en consideración para determinar la existencia de un nivel adecuado de protección en las transferencias internacionales de datos personales según se fundamenten en decisiones de adecuación o en cláusulas contractuales tipo, otorgando una diferente eficacia a normas de idéntica naturaleza jurídica como son las decisiones de la Comisión.

En todo caso, el Tribunal de Justicia aclara que el carácter no vinculante respecto de las autoridades del tercer país que atañe a la Decisión de la Comisión 2010/87/UE (Decisión CPT) "no afecta a la validez" de la misma que, por el contrario, depende de la previsión de mecanismos que garanticen el respeto de los estándares de protección exigidos por la Unión -sin hacer expresa referencia al art. 45.2 RGPD-, interpretados según los arts. 7, 8 y 47 de la Carta de los Derechos Fundamentales, y del hecho de que las transferencias de datos basadas en dichas cláusulas tipo puedan ser suspendidas o prohibidas si no se pueden respetar tales garantías o estas resultan de imposible cumplimiento (pars. 136-137).

Concretamente, el TJUE considera que la Decisión 2010/87/CE (Decisión CPT) obliga al exportador de los datos y al destinatario de la transferencia («importador de los datos») a comprobar con carácter previo que el nivel de protección exigido en la UE se respeta en el país tercero de que se trate (operación que se lleva a cabo por remisión a los arts. 7, 8 y 47 CDFUE y no a los elementos enunciados en el art. 45.2 RGPD), y también exige al importador de los datos que informe al exportador de que podría ser incapaz de cumplir las cláusulas tipo de protección de datos, en cuyo caso el exportador de los datos deberá suspender la transferencia de datos o rescindir el contrato suscrito con el importador (pars. 141-146).

La concurrencia de ambas exigencias conduce al Tribunal de Justicia a reconocer la validez de la Decisión CPT (par. 149), aunque siguiendo las indicaciones contempladas en el Considerando 109 RGPD, estima recomendable que las transferencias internacionales de datos basadas en cláusulas contractuales tipo se incluyan en "un contrato más amplio" como sería un contrato entre dos encargados, o bien "se añadan otras cláusulas o garantías adicionales" mediante compromisos contractuales que sirvan de complemento a las cláusulas contractuales tipo de protección de datos (par. 109). De ahí que, en última instancia, aliente a los responsables del tratamiento de los datos a ofrecer garantías adicionales "que complementen" las cláusulas tipo de protección de datos (par. 132).

4.3. El cumplimiento por el Escudo de Privacidad del nivel de protección sustancialmente equivalente al establecido en el Derecho de la Unión

El TJUE se pronuncia acerca del grado de vinculación de las autoridades nacionales de control respecto de las diferentes constataciones contenidas en la Decisión de Ejecución 2016/1250 (Decisión EP) que sirven a la Comisión para alcanzar la conclusión, reconocida expresamente en su art. 1.1, de que los EEUU garantizan un nivel de protección adecuado a los efectos del art. 45.1 RGPD.

Una verificación que se llevó a cabo por la Comisión desde la premisa de que el Escudo de Privacidad está integrado tanto por los principios establecidos por el Departamento de Comercio de los Estados Unidos el 7 de julio de 2016 (Anexo II de la Decisión EP), como por los compromisos y declaraciones oficiales (Anexos I, III a VII de la Decisión EP) aun cuando el punto I.5 del Anexo II reconozca que la adhesión a tales principios puede verse limitada, entre otros motivos, por exigencias de seguridad nacional, interés público y cumplimiento de la Ley.

La previsión en la Decisión de Ejecución 2016/1250 de dicha limitación conduce al TJUE, siguiendo el criterio establecido en el asunto *Schrems I*, a considerar que la primacía otorgada por el Escudo de Privacidad a las exigencias de seguridad nacional, interés público y complimiento de la ley es-

tadounidense tiene "carácter general", posibilitando injerencias por parte de las autoridades públicas norteamericanas en los derechos fundamentales de las personas cuyos datos se transfieren a través de los programas de vigilancia *PRISM* y *UPSTREAM* (par. 165).

No obstante, habida cuenta de que el Considerando 140 de la Decisión EP exige que las intromisiones de los poderes públicos de los EEUU "se limitarán" a lo estrictamente necesario para alcanzar el objetivo legítimo perseguido y pueden ser tuteladas efectivamente por los tribunales, el TJUE debe entrar a valorar la normativa estadounidense reguladora de tales programas de vigilancia a los efectos de comprobar si ofrece un nivel de protección adecuado.

Dos aspectos esenciales que, según afirma el TJUE, forman parte de lo que denomina el "nivel de protección exigido" por el Derecho de la Unión (par. 165), cuya evaluación debe tomar en consideración el principio de proporcionalidad al que alude el art. 52.1 CDFUE respecto de las limitaciones de los derechos y libertades, y el reconocimiento a los ciudadanos europeos cuyos datos son objeto de transferencia, de la tutela judicial efectiva para el supuesto de que sus derechos fundamentales resulten vulnerados según establece el art. 47 CDFUE.

Aplicando estos criterios al procedimiento en cuestión el TJUE estima que la normativa estadounidense analizada no define por sí misma "el alcance de la limitación" del ejercicio del derecho de los derechos de los interesados, ni establece "reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas" (pars. 178-179).

Unas carencias a las que el TJUE otorga una especial relevancia, alcanzando la conclusión de que las limitaciones del derecho a la protección de datos que se derivan de la normativa interna de los Estados Unidos en virtud de la cual se permite el acceso y la utilización por las autoridades estadounidenses de los datos transferidos a los EEUU, "no están reguladas" de acuerdo con las exigencias sustancialmente equivalentes establecidas por el Derecho de la Unión y, en concreto, por el principio de proporcionalidad al que alude el art. 52.1, segunda frase de la CDFUE (pars. 181-185).

Por lo que respecta al derecho a la tutela judicial efectiva, considerado por el TJUE como el segundo elemento que conforma el nivel de protección exigido dentro de la Unión, el análisis pormenorizado de la normativa estadounidense pone de manifiesto que "no confiere" a los ciudadanos europeos derechos exigibles a las autoridades estadounidenses ante los tribunales (par. 182).

En consecuencia, a juicio del Alto Tribunal de la UE, una normativa que no prevé posibilidad alguna de que el interesado pueda ejercer acciones en Derecho para el acceso a los datos personales que le conciernen y, en su caso, solicitar su rectificación o supresión, a juicio del Alto Tribunal de la UE "no respeta el contenido esencial" del derecho fundamental a la tutela efectiva reconocido en el art. 47 CDFUE (par. 187).

No obstante, la exigencia al tercer país por el Considerando 104 RGPD de garantizar la existencia de un control "verdaderamente independiente" de la protección de datos, que reconozca a los interesados "derechos efectivos y exigibles" y "acciones administrativas y judiciales efectivas", conduce al TJUE a analizar la figura del Defensor del Pueblo cuya creación en los EEUU viene contemplada por la Decisión EP (par. 188).

De este modo, el TJUE procede a analizar si la configuración jurídica del Defensor del Pueblo en la legislación norteamericana y sus competencias respecto de las garantías de los derechos de los ciudadanos europeos cuyos datos son objeto de transferencia a los EEUU, cumple los criterios de garantía del art. 47 CDFUE exigidos por el ordenamiento de la Unión en el marco de las transferencias internacionales de protección de datos.

A resultas del examen de tales aspectos el Alto Tribunal de la UE estima que ni la "naturaleza de la misión encomendada" a dicho órgano en calidad de "coordinador superior de la diplomacia internacional en materia de tecnología de la información" le otorga facultades para adoptar "decisiones vinculantes" con respecto a los servicios de inteligencia estadounidenses, ni existe garantía legal de que pueda hacerlo (pars. 193, 196). Además, entiende que tampoco existen garantías adecuadas de su independencia respecto del Poder ejecutivo, habida cuenta de que el Defensor del Pueblo es designado por el Secretario de Estado y se integra en el organigrama administrativo del Departamento de Estado. Tales constataciones le permiten concluir, en última instancia, que el Defensor del Pueblo no proporciona ninguna "vía de recurso" ante un órgano que ofrezca a las personas cuyos datos se transfieren a los EEUU garantías sustancialmente equivalentes a las exigidas por el art. 47 CDFUE (pars. 195-197).

Como conclusión de su análisis en el asunto *Schrems II* el TJUE entiende que el art. 1.1 de la Decisión de adecuación 2016/1250 (Decisión EP) al reconocer que "los Estados Unidos garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión a entidades establecidas en los Estados Unidos en el marco del Escudo de la privacidad", no tuvo en cuenta los elementos contenidos en el art. 45.1 RGPD interpretado a la luz de los arts. 7, 8 y 47 de la Carta y, en consecuencia, es inválido. Una invalidez que el Alto Tribunal de la Unión extiende al conjunto de la Decisión de Ejecución 2016/1250 (Decisión EP) habida cuenta de la conexión indisociable de dicho precepto con los artículos 2 a 6 y los Anexos (pars. 199-200)[30].

[30] Cabe subrayar que tanto en la consideración de algunas de las cuestiones prejudiciales remitidas por el Tribunal Superior irlandés como en la declaración de invalidez de la Decisión de Ejecución 2016/1250 (Decisión EP), el TJUE se aparta de las apreciaciones del Abogado General Sr. Henrik Saugmandsgaard Øe en el asunto *Schrems II*.

Efectivamente, según el criterio del Abogado General no existe necesidad de responder a las cuestiones prejudiciales Segunda a Quinta, ni a la Décima, ni cree conveniente que el TJUE se pronuncie sobre la validez de la Decisión 2016/1250 sobre el

CONCLUSIONES

La importancia de las relaciones UE-EEUU ha llevado a la Comisión Europea a implementar desde 1999 dos marcos normativos distintos y sucesivos que hicieran posible la transferencia de datos personales de uno a otro lado del Atlántico garantizando el cumplimiento en los Estados Unidos como tercer país, de los estándares de protección de la Unión respecto de los derechos a la vida privada, a la protección de datos personales (arts. 7 y 8 CDFUE) y del derecho a la tutela judicial efectiva respecto de los mismos (art. 47 CDFUE).

Al igual que hiciera en el asunto *Schrems I* en relación con el sistema de Puerto Seguro, en la Sentencia de 16 de julio de 2020 asunto *Schrems II*, el TJUE ha vuelto a posicionarse como "juez garante de la privacidad en Internet" (Rallo Lombarte, 2017, 583), estimando insuficientes las garantías establecidas para la transferencia de datos personales de los ciudadanos europeos en el Escudo de Privacidad (*Privacy Shield*).

Una apreciación que tiene como consecuencia la declaración de invalidez de la decisión de adecuación (Decisión de Ejecución 2016/1250-Decisión EP) adoptada por la Comisión como base jurídica para llevar a cabo las transferencias de datos entre la UE y los EEUU, desde la premisa de que "la protección otorgada a los datos personales en el Espacio Económico Europeo (EEE) debe viajar con los datos donde estos vayan" (CEPD-EDPB 2020b, p. 2).

Ciertamente, continuando la línea iniciada en el asunto *Schrems I*, en *Schrems II* el TJUE reitera de modo contundente la imposibilidad de que la decisión de adecuación adoptada por la Comisión europea en la que verifica el nivel adecuado de protección de los datos personales en el tercer país otorgue primacía, con carácter general, a las exigencias de seguridad nacional e interés público que impliquen una injerencia ilegítima de sus autoridades públicas en los derechos fundamentales de los ciudadanos europeos cuyos datos son objeto de la transferencia.

De este modo, al igual que desde 1978 viene haciendo el TEDH (asunto *Klass and Others v. Germany*), gracias a los asuntos *Schrems I y II* el Alto Tribunal de la UE se suma a la "tarea de someter a Derecho" también las actividades de los servicios de inteligencia y aquellas dirigidas a prevenir y

---

Escudo de Privacidad (Decisión EP) habida cuenta de que "el órgano jurisdiccional remitente no ha planteado de forma explícita" sino indirectamente la cuestión de la validez de esta última (par. 165).

Además, respecto de la Decisión 2010/87/UE (Decisión CPT) considera que los argumentos que pueda aportar el Alto Tribunal de la UE sobre las cuestiones prejudiciales planteadas "no pueden afectar a su conclusión relativa a la validez *in abstracto* de la Decisión 2010/87 ni, por tanto, influir en la resolución del litigio principal". No obstante, reconoce que la formulación de aclaraciones sobre dichas cuestiones podría ayudar a la autoridad de control nacional a valorar si procede la "suspensión in concreto" de las transferencias de datos implicadas por falta de garantías adecuadas.

combatir el terrorismo mediante la aplicación de criterios de proporcionalidad (Lucas Murillo de la Cueva, 2020, p. 6).

En efecto, en ambos pronunciamientos el TJUE lleva a cabo una ponderación acerca del grado de injerencia admisible por parte de las autoridades públicas del tercer país en los derechos reconocidos en los arts. 7, 8 y 47 (CDFUE), de la que se desprende la existencia de un contenido esencial del derecho a la protección de datos personales que debe ser garantizado cuando los datos personales de los ciudadanos europeos son objeto de una transferencia internacional.

Pero además, a instancia de la High Court (Tribunal Superior de Irlanda), en el asunto *Schrems II* el TJUE tiene la oportunidad de llevar a cabo una labor hermenéutica que por primera vez toma como referencia directa el RGPD para sentar las bases del nivel de protección sustancialmente equivalente al exigido por la Unión respecto de las transferencias de datos realizadas mediante cláusulas contractuales tipo de protección de datos, y aquí es, precisamente, donde el Alto Tribunal de la UE queda muy lejos de las expectativas.

En efecto, el pronunciamiento del Tribunal de Justicia en el asunto *Schrems II* es el resultado de un *iter* argumentativo con muchas aristas que no puede ser considerado un modelo de sistemática, claridad y congruencia en la exposición de sus razonamientos.

Pero no todo está perdido en el laberinto normativo y en la profusa acronimia en que nos sumerge el TJUE en el asunto *Schrems II*. El aspecto más relevante y novedoso que cabe encontrar en dicho pronunciamiento proviene de la equiparación que lleva a cabo, con carácter general, entre el nivel de garantía exigido a las decisiones de adecuación adoptadas por la Comisión de acuerdo con el art. 45 RGPD y a las realizadas en virtud de las cláusulas tipo de protección de datos previstas en el art. 46.2 RGPD, debiendo en ambos supuestos valorarse en el tercer país los elementos enunciados en el art. 45.2 RGPD (par. 105).

Ello implica que las cláusulas contractuales tipo adoptadas por la Comisión también deben evaluar aspectos tales como la vigencia del Estado de Derecho, el respeto de los derechos humanos, el análisis de la legislación pertinente, tanto general como sectorial, las medidas de seguridad aplicadas a la protección de datos, la jurisprudencia del tercer país. Pero, especialmente, la tutela judicial efectiva de los interesados cuyos datos sean objeto de transferencia, el funcionamiento efectivo de autoridades independientes de protección de datos, y los compromisos internacionales asumidos por el tercer país.

Esta homologación de las garantías, en principio, dificultaría la utilización de las cláusulas contractuales tipo como medio para eludir el nivel de protección exigido por la normativa europea a las transferencias basadas en decisiones de adecuación. Sin embargo, cuando el Alto Tribunal de la UE entra a examinar el nivel de protección de los datos objeto de transferencia desde la UE a los EEUU en aplicación de la Decisión de la Comisión 2010/87/CE (Decisión CPT) que recoge las cláusulas contractuales tipo, no se mencio-

na de modo explícito la toma en consideración de los elementos enunciados en el art. 45.2 RGPD.

Por el contrario, el Tribunal de Justicia estima que la validez de la Decisión 2010/87/UE (Decisión CPT) depende de la previsión de mecanismos que garanticen el respeto de los estándares de protección exigidos por la Unión interpretados de acuerdo con la CDFUE, y del hecho de que las transferencias internacionales de datos basadas en dichas cláusulas tipo puedan ser suspendidas o prohibidas si no se pueden respetar tales garantías o estas resultan de imposible cumplimiento, sugiriendo la necesidad de promover conductas más protectoras mediante la incorporación de garantías adicionales de protección de datos.

De este modo, la imagen gráfica que el Alto Tribunal de la UE diseña en el asunto *Schrems II* respecto de las transferencias internacionales de datos personales basadas en cláusulas contractuales tipo, consiste en la concepción de un acuerdo de transferencia internacional de datos personales de carácter amplio. Este contrato incluiría no solo las cláusulas tipo adoptadas por la Comisión o una autoridad de control, sino también un conjunto de garantías adicionales de protección de los datos personales respecto de las cuales la única concreción que aporta consiste en la exigencia de que resulten vinculantes para el tercer país.

Por ello, como certeramente formula Lucas Murillo de la Cueva (2020), la pregunta que nos asalta cuando concluimos la lectura del pronunciamiento del TJUE en el asunto *Schrems II* es: "¿y ahora qué?" (p. 9).

La respuesta a esta pregunta la viene apuntando el Comité Europeo de Protección de Datos en distintos documentos publicados con posterioridad al asunto *Schrems II*, como las "Preguntas frecuentes sobre la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-311/18-Comisaria de Protección de Datos *vs*. Facebook Irlanda y Maximillian Schrems" (2020a), y las Recomendaciones sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de datos personales de la UE (2020b) donde, a la espera de un análisis pormenorizado de dicho pronunciamiento, aclara que a partir del mismo resultan ilegales las transferencias de datos personales basadas en la decisión de adecuación 2016/1250 (Decisión EP).

No obstante, el CEPD-EDPB reconoce que desde ese momento resulta aceptable la utilización de las excepciones previstas en el art. 49 RGPD para llevar a cabo las transferencias de datos, supeditándolas al cumplimiento de los términos contemplados en las Directrices sobre esta disposición, que imponen la premisa de limitar su aplicación de modo ocasional y no repetitivo (Directrices 2/2018). Pero también admite la posibilidad de utilizar las cláusulas contractuales tipo de protección de datos siempre que sean evaluadas caso por caso atendiendo a las circunstancias de las transferencias -sin concretar los parámetros de evaluación ni las circunstancias-, y a las medidas complementarias adoptadas.

En este sentido, ante la ausencia de una decisión de adecuación adoptada por la Comisión que tome en consideración el cumplimiento en el tercer país de los elementos enunciados en el art. 45.2 RGPD, la opción indicada por el CEPD-EDPB de supeditar las transferencias UE-EEUU basadas en cláusulas contractuales tipo a la valoración de las garantías adecuadas, caso por caso, sobre criterios tan imprecisos, junto a la traslación de la decisión sobre el cumplimiento de las mismas al responsable *ad hoc* de la transferencia en la Unión no parece responder a las exigencias mínimas de garantía aplicables a la protección de los datos personales de los ciudadanos europeos.

Ciertamente, la tenacidad del Sr. Schrems ha llevado por dos veces al TJUE a pronunciarse respecto de las transferencia de datos personales entre la UE y los EEUU, y el Alto Tribunal de la UE ha emitido en ambos casos resoluciones garantistas con respecto a los derechos contemplados en los arts. 7, 8 y 47 CDFUE. Sin embargo, en *Schrems II* el Tribunal de Justicia deja una espita abierta que podría suponer el desarrollo de las transferencias de datos personales eludiendo el nivel de garantías exigido por la Unión a los terceros países y sin una aplicación homogénea en los Estados miembros.

Por ello, si el CEPD-EDPB afirma que la premisa de la que parte el TJUE en el asunto *Schrems II* consiste en considerar que en las transferencias de datos personales las garantías viajan allá donde van los datos, también cabría entender que, en ocasiones, puede que estos pierdan el equipaje.

FUENTES CITADAS

A. Bibliografía

Álvarez Rigaudias, C. (2012). Condiciones para las transferencias internacionales de datos personales en servicios de *cloud*. En R. Martínez Martínez (ed.), *Derecho y cloud computing*. Aranzadi (109-147).

Adsuara, B. (2019). Derechos de rectificación, supresión (olvido) y portabilidad (de los datos) y de limitación y oposición (al tratamiento). En A. Rallo Lombarte (dir.), *Tratado de protección de datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*. Tirant lo Blanch (313-352).

Blanc, N. (2017). Schrems v. Facebook: Jurisdiction Over Consumer Contracts Before the CJEU. *European Data Protection Law Review*, 3, 413-417 (DOI: 10.21552/edpl/2017/3/20).

Castellanos Rodríguez, A. (2017). El régimen jurídico de las transferencias internacionales de datos personales. Especial mención al marco regulatorio Privacy Schield. *Institut de Ciències Polítiques i Socials (UAB)*, WP 350.

Comella, C. (2015). Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa, a margine della sentenza "Safe Harbor" della Corte di Giustizia dell'Unione Europea. *Diritto dell'informazione e dell'informatica*, 31 (4-5), 131-136.

Comisión Europea (2013a). *Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE* (COM(2013) 847 final) (27 de nov. de 2013).

— (2013b). *Comunicación de la Comisión al Parlamento Europeo y al Consejo. Restablecer la confianza en los flujos de datos entre la UE y EE.UU* [COM (2013) 846 final] (27 de nov. de 2013).
— (2017a). *Comunicación de la Comisión al Parlamento Europeo y al Consejo. Intercambio y protección de los datos personales en un mundo globalizado* [COM(2017) 7 final] (10 de ene. de 2017).
— (2017b). *Informe de la Comisión al Parlamento Europeo y al Consejo sobre la primera revisión anual del funcionamiento del Escudo de privacidad UE-EEUU* [COM(2017 611 final] (18 oct. 2017).
— (2018). *Informe de la Comisión al Parlamento Europeo y al Consejo sobre la revisión anual del funcionamiento del Escudo de la privacidad UE-EEUU* [COM(2018) 860 final] (19 de dic. de 2018).
— (2019a). *Comunicación de la Comisión al Parlamento Europeo y al Consejo. Balance de las normas de protección de datos como catalizador de la confianza de la UE y fuera de sus fronteras* [COM(2019) 374 final] (24 de jul. de 2019).
Comisión Europea (2019b). *Informe de la Comisión al Parlamento Europeo y al Consejo sobre la tercera revisión anual del funcionamiento del Escudo de la privacidad UE-EEUU* [COM(2019) 495 final] (23 de oct. de 2019).
Comité Europeo de Protección de Datos. *Directrices 2/2018 sobre las excepciones contempladas en el artículo 49 del Reglamento 2016/679* (25 de may. de 2018).
— (2020a). *Preguntas frecuentes sobre la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-311/18-Comisaria de Protección de Datos vs Facebook Irlanda y Maximillan Schrems. Adoptada el 23 de julio de 2020* (24 de jul. de 2020).
Constant, B. (1819). De la liberté des anciens comparée à celle des modernes. Discours prononcé à l'Athénée royal de Paris en 1819. En, Constant, B. (1997). Écrits *politiques. Textes choisis, présentés et annotés par Marcel Gauchet*. Gallimard.
Cordero Álvarez, C. I. (2019). La transferencia internacional de datos con terceros Estados en el nuevo Reglamento Europeo: Especial referencia al caso estadounidense y la Cloud Act. *Revista Española de Derecho Europeo*, 70, 49-108.
Coudray, L. (2004). Case C-101/01, Bodil Lindqvist. *Common Market Law Review*, 41(5), 1361-1376.
Data Protection Party on the Protection of Individuals with Regard to the Processing of Personal Data (2000). *Opinion 3/2000, on the EU/US dialogue concerning the "Safe harbor" arrangement* (WP 32). (5019/00/EN/Final).
Data Protection Party on the Protection of Individuals with Regard to the Processing of Personal Data. European Commission (2015). *Statement of the Article 29 Working Party on Schrems Judgement* (16 de oct. de 2015).
Data Protection Party on the Protection of Individuals with Regard to the Processing of Personal Data (2016). *Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)*. (WP 237) (13 de abr. de 2016).
Data Protection Party on the Protection of Individuals with Regard to the Processing of Personal Data (2016). *Opinion 01/2016, on the EU-US Privacy Shield draft adequacy decision*. (WP 238) (13 de abr. de 2016).
Data Protection Party on the Protection of Individuals with Regard to the Processing of Personal Data (2017). *EU-US Privacy Shield-First annual Joint Review.* (WP 255) (28 de nov. de 2017).
Data Protection Party on the Protection of Individuals with Regard to the Processing of Personal Data. European Commission (2018). *Working Document: Transfers of personal data to third countries: Applying Article 25 and 26 of the EU data protection directive* (WP 12). (DG XV D/505/98).

Data Protection Party on the Protection of Individuals with Regard to the Processing of Personal Data (2019). *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*. (WP 168) (1 de dic. de 2019).

De Miguel Asensio, P. A. (2015). Aspectos internacionales de la protección de datos: las sentencias Schrems y Weltimmo del Tribunal de Justicia. *La Ley Unión Europea*, 31, 1-10.

European Data Protection Board (2020). *Guidelines 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 (15 de dic. de 2020).

— (2020b). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with EU level of protection of personal data*. (10 nov. 2020).

European Data Protection Supervisor (2016). *Opinion on the EU-U.S. Privacy Shield draft adequacy decision* (30 de may. de 2016).

Gömann, M. (2017). The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement. *Common Market Law Review*, 54, 567-590.

Gonzalo Domenech, J. J. (2019). 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*, 11(1), pp. 350-371. DOI: https://doi.org/10.20318/cdt.2019.4624.

Kuner, Ch. (2017). Reality and Illusion in EU Data Transfer Regulation Post Schrems. *German Law Journal*, 18(4), 881-918.

Lam. C. (2017). Unsafe Harbor: The European Union's demand for heightened data privacy standards in Schrems v. Irish Data Protection Commissioner. *Boston College International & Comparative Law Review, 40: E. Supp.*, 1-13.

López Aguilar, J. F. (2017). La protección de datos personales en la más reciente jurisprudencia del TJUE: Los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EEUU. *UNED. Teoría y Realidad Constitucional*, 39, 557-581. DOI: https://doi.org/10.5944/trc.39.2017.19165.

Lowe, D. (2016). The European Union's Passenger Name Record Data Directive 2016/681: Is It Fit for Purpose? *International Criminal Law Review*, 16(5), 856-884.

Lucas Murillo de la Cueva, P. (1990). *El derecho a la autodeterminación informativa*. Tecnos.

— (2003). La Constitución y el derecho a la autodeterminación informativa. *Cuadernos de Derecho Público*, 19-20, 27-43.

— (2020). Entrevista: El perpetuum mobile del derecho a la protección de datos: no solo mantenerlo, sino reforzarlo. *La Ley Privacidad*, 6, 1-16.

McGinnis, B. J. y Miller, B. W. (2015). European Court of Justice Invalidates US-EU Safe Harbor Agreement. *National Law Review* (https://www.natlawreview.com/article/european-court-justice-invalidates-us-eu-safe-harbor-agreement).

Mendez, M. (2007). Passenger Name Record Agreement. European Court of Justice. Annulment of Commission Adequacy Decision and Council Decision Concerning Conclusion of Passenger Name Record Agreement with US Grand Chamber Judgement of 30 May 2006, Joined cases C-317/04 and C-318/04, European Parliament v. Council and Commission. *European Constitutional Law Review*, 3, 127-147.

Meyer, J. E. Foreign Companies: Does the U.S. Government Now Have Access to Your Overseas Data? *The National Law Review* (4 de dic. de 2018) (https://www. natlawreview.com/article/ foreign-companies-does-us-government-now-have-access-to-your-overseas-data).

Núñez García, J. L. (2019). Responsabilidad y obligaciones del responsable y del encargado del tratamiento. En A. Rallo Lombarte (dir.), *Tratado de protección de da-*

tos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. Tirant lo Blanch (353-386).

Ortega Giménez, A. y Gonzalo Domenech, J. J. (2018). Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea. *Revista de la Facultad de Derecho*, 44, 1-35 (http://dx.doi.org/10.22187/rfd2018n44a2).

Parlamento Europeo (2014). *Resolución [P7_TA(2014)0230], sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EEUU, los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de justicia y asuntos de interior* [2013/2188/(INI)]. (12 de mar. de 2014).

— (2018a). *Resolución [P8_TA(2018)0315], sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU. (2018/2645(RSP))*(5 de jul. de 2018).

— (2018b). *Resolución [P8_TA(2018)0433], sobre la utilización de los datos de los usuarios de Facebook por parte de Cambridge Analytica y el impacto en la protección de los datos (2018/2855/(RSP))* (25 de oct. de 2018).

— (2019). *Resolución [P8_TA(2019)0142], sobre la propuesta de Decisión del Consejo por la que se autoriza a los Estados miembros a firmar, en interés de la Unión Europea, el Protocolo que modifica el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (10923/2018- C8-0440/2018- 2018/0238(NLE))* (12 de mar. de 2019).

Pérez Francesch, J. L.; Gil Márquez, T., y Gacitúa Espósito, A. (2011). Informe sobre el PNR. La utilización de datos personales contenidos en el registro de nombres de pasajeros: ¿fines represivos o preventivos? *Working Papers, núm. 297*. Institut de Ciències Polítiques i Socials.

Piñar Mañas, J. L. (2016). XXV. Transferencias de datos personales a terceros países y organizaciones internacionales. En Piñar Mañas, J. L. (dir.). *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Ed. Reus.

Poullet, Y. (2007). Flujos de datos transfronterizos y extraterritoriales: la postura europea. *Revista Española de Protección de Datos*, 1, 93-113.

Puerto, M.ª I. y Taibi, P. S. (2018). La Sentencia *Schrems* del Tribunal de Justicia de la Unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva internacional. *Revista Derecho del Estado*, 40, 209-236.

Rallo Lombarte, A. (2017). El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en Internet. *UNED. Teoría y Realidad Constitucional*, 39, 583-610.

Roth, P. (2017). "Adequate level of data protection" in third countries post-*Schrems* and under the General Data Protection Regulation. *Journal of Law, Information and Science*, 25(1), 55-67.

Simon, D. (2020). Coup de tonnerre dans le monde du numérique. La Cour de Justice prononce l'invalidité du "bouclier de protection de la vie privée" à propos des transferts de données personnelles vers les États-Unis. *Europe: actualité du droit communautaire*, 30 (8-9), 5-10.

Svantesson, D. J. B. (2014). The Extraterritoriality of EU Data Privacy Law-Its theoretical Justification and its practical Effect on U.S. Businesses. *Stanford Journal of International Law*, 50, 53-67.

— (2016). Cross-Border data transfers after the CJEU's Safe Harbour Decision. A tale of Gordian knots. *Alternative International Journal*, 41(1), 39-42.

Syed, H. y Yilmaz Genç, S. (2019). European Union General Data Protection Regulation (GDPR) and United States of America's clarifying overseas use of Data (Cloud) Act: David versos Goliath. En, Yilmaz Genç, S. y Demir, S. (eds.), *V. European Congress on Economic Issues. Proceedings Book*. Pazıl Reklam Danışmanlık Matbaa ve Organizasyon Ltd.Sti.

The Sunday Business Post. https://www.businesspost.ie/legal/facebook-fears-ruling-may-force-it-to-pull-social-media-platforms-from-eu-00644da4.

Uría Gavilán, E. (2016). Derechos fundamentales *versus* vigilancia masiva. Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 Schrems. *Revista de Derecho Comunitario Europeo*, 53, 261-282.

Ustarán, E. y García, P. (2019). Transferencias internacionales de datos. En A. Rallo Lombarte (dir.), *Tratado de protección de datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*. Tirant lo Blanch (459-490).

Van Alsenoy, B. (2016). Liability under EU Data Protection Law. From Directive 95/46 to the General Data Protection Regulation. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 7(3), 271-288.

Voss, W. G. (2016). European Union Data Privacy Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting. *Business Layer*, 72(1), 221-234.

VV.AA. (2020). *UNED. Teoría y Realidad Constitucional*, 46, pp. 15-118.

Zhao, B. y Chen, W. (2019). Data Protection as a Fundamental Right: The European General Data Protection Regulation and Its Exterritorial Application in China. *US-China Law Review*, 16(3), 97-113.

B. Legislación y jurisprudencia

Conclusiones AG Sr. Henrik Saugmandsgaard Øe (2020). *Schrems II*, C-311/18. ECLI:EU:C:2019:1145.

Consejo de Europa (1981). Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. *BOE* núm. 274 (15 de nov. de 1985).

— (2018). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as it will be amended by its Protocol CETS núm. 223. Texto consolidado disponible en: https://rm.coe.int/16808ade9d.

Decisión (2000/520/CE) de la Comisión, de 26 de julio de 2000, *con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América*. *DOCE* L 215 (25 de ago. de 2000).

Decisión (2001/497/CE) de la Comisión, de 15 de junio de 2001, *relativa a las cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE. DOCE* L 181 (4 de jul. de 2001).

Decisión (2004/915/CE) de la Comisión, de 27 de diciembre de 2004, *por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países*.

DOCE L 385 (29 de dic. de 2004).

Decisión (2006/230/CE) del Consejo, de 18 de julio de 2005, *relativa a la celebración de un acuerdo entre la Comunidad Europea y el Gobierno de Canadá sobre el tratamiento de datos API/PNR*. *DOUE* L 82 (21 de mar. de 2006).

Decisión (2006/253/CE) de la Comisión, de 6 de septiembre de 2005, *relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros (Passenger Name Records, PNR) que se transfieren a la Canada Border Services Agency (Agencia de Servicios de Fronteras de Canadá)*. *DOUE* L 91 (29 de mar. de 2006).

Decisión (2004/535/CE) de la Comisión, de 14 de mayo de 2004, *relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos*. *DOUE* L 235 (6 de jul. de 2004).

Decisión (2007/551/PESC/JAI) del Consejo, de 23 de julio de 2007, *relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (Acuerdo PNR 2007)*. *DOUE* L 204 (4 de ago. de 2007).

Decisión (2012/471/UE) del Consejo, de 13 de diciembre de 2011, *relativa a la firma, en nombre de la Unión, del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos* (Acuerdo PNR 2012). *DOUE* L 215 (11 de ago. de 2012).

Decisión (2012/472/UE) del Consejo, de 26 de abril de 2012, *relativa a la celebración del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos* (Acuerdo PNR 2012). *DOUE* L 215 (11 de ago. de 2012).

Decisión (2010/87/UE) de la Comisión, de 5 de febrero de 2010, *relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo*. *DOUE* L 39 (12 de feb. de 2010).

Decisión de Ejecución (UE) 2016/1250, de la Comisión, de 12 de julio de 2016, *con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU*. *DOUE* L 207 (1 de ago. de 2016).

Decisión de Ejecución (UE) 2016/2297, de la Comisión, de 16 de diciembre de 2016, *por la que se modifican las Decisiones 2001/497/CE y 2010/87/UE, relativas a las cláusulas contractuales tipo para las transferencias de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo. DOUE* L 344 (17 de dic. de 2016).

Decisión (UE) 2016/920, del Consejo, de 20 de mayo de 2016, *sobre la firma, en nombre de la Unión Europea, del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la protección de los datos personales en relación con la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales*. *DOUE* L 154 (11 de jun. de 2016).

Department of Homeland Security (2015). Office of Intelligence and Analysis. Policy Instruction: IA-1002. *Safeguarding Personal Information Collected from Signals Intelligence Activities* as required by Presidential Policy Directive 28- PPD-28 (16 de ene. de 2015).

Dictamen TJUE (2015). *Acuerdo PNR UE-Canadá* (26 jul. 2017). ECLI:EU:C:2017:592.

Directiva 95/46/CE, del Parlamento Europeo y el Consejo, de 24 de octubre de 1995, *relativa a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. *DOCE* L 281 (23 de nov. de 1995).

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 la libre circulación de dichos datos, y por la que se deroga la Decisión 2008/977/JAI*. *DOUE* L 119 (4 de may. de 2016).

Directiva (UE) 2016/681, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, *relativa a la utilización de datos del registro de nombres de los pasajeros (PNR), para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave*. *DOUE* L 119 (4 de may. de 2016).

Executive Order 13768, *Enhancing Public Safety in the Interior of the United States*. Federal Register 2017-02102 (30 de ene. De 2017).

Public Law 115-141. 115th Congress. *Consolidated Appropriation Act, 2018.* Section 105. H.R. 1625 (House of Representatives 4943) (23 de mar. de 2018).

Public Law 115-141. 115th Congress. H.R. 4943. Division V. *Clarifying Lawful Overseas Use of Data Act - Cloud Act* (23 de mar. de 2018).

Public Law 114-126. 114th Congress. *Judicial Redress Act of 2015*. USC 552a note (24 de feb. de 2016).

Public Law 115-22. 115th Congress (S.J. Res. 34). *Joint Resolution Providing for congressional disapproval under chapter 8 of title 5. United States Code, of the rule submitted by the Federal Communications Commission relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services'* (3 de abr. de 2017).

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). *DOUE* L 119 (4 de may. de 2016).

Sentencia BVerG, 1 BvR 209/83. BVerGE 65, 1-71 (15 de dic. de 1983) (versión inglesa).

Sentencia High Court Ireland. *The Data Protection Commissioner & Facebook Ireland Limited & Maximillian Schrems*. [2017] IEHC 545 (3 de oct. de 2017).

Sentencia Tribunal Superior Regional de Viena (*Oberlandesgericht*). *Maximilian Schrems v. Facebook Ireland Limited*.11 R2153/20f, 154/20b (28 de dic. de 2020) (versión inglesa).

Sentencia TC 254/1993 (20 de jul. de 1993). ECLI:ES:TC:1993:254.

Sentencia TC 292/2000 (30 de nov. de 1993). ECLI:ES:TC:2000:292.

Sentencia TEDH. (1978). *Klass and Others v. Germany* (6 sept. 1078). App. n. 5029/71.

Sentencia TEDH. (2000). *Amann v. Switzerland* (16 de feb. de 2000). App. n. 27798/95.

Sentencia TEDH. (2000). *Rotaru v. Romania* (4 de may. de 2000). App. n. 28341/95.

Sentencia TJUE. (2003). *Bodil Lindqvist*, C- 101/01. ECLI:EU::2003:596.

Sentencia TJUE. (2003). Österrichischer *Rundfunk y otros*, asuntos acumulados C-465/00, C-138/01 y C-139/0. EU:C:2003:294.

Sentencia TJUE. (2006). *Parlamento v. Consejo y Comisión*, C-317/04 y C-318/04. EU:C:2006:346.

Sentencia TJUE. (2009). *Rijkeboer*, C-553/07. EU:C:2009:293.

Sentencia TJUE. (2010). *Volker und Markus Schecke v. Eifert*, asuntos acumulados C-92/09 y C-93/09. EU:C:2010:662.

Sentencia TJUE. (2014). *Digital Rights Ireland y otros,* asuntos acumulados C-293/12 y C-594/12. EU: C:2014:238.

Sentencia TJUE. (2014). *Google Spain v. Google*. C-131/12. ECLI:EU:C:2014:317.

Sentencia TJUE. (2015). *Schrems*. C-362/14. ECLI:EU:C:2015:650.

Sentencia TJUE. (2015). *František Ryneš*. C-212/13. ECLI:EU:C:2014:2428.

Sentencia TJUE. (2016). *Recurso La Quadrature du Net y otros v. Comisión.* T-738/16 (2017/ C 006/49) (25 de oct. de 2016).

Sentencia TJUE. (2017). *Puškár*. C-73/16. ECLI:EU:C:2017:725.

Sentencia TJUE. (2017). *Bolagsupplysningen e Ilsjan*. C-194/16. ECLI:EU:C:2017:766.

Sentencia TJUE. (2018). *Jehovan todistajat*. C-25/17. ECLI:EU:C:2018:551.

Sentencia TJUE. (2019). *Google LLC y Commission nationale de l'informatique et des libertés (CNIL)*. C-507/17. ECLI:EU:C:2019:772.
Sentencia TJUE. (2020). *Data Protection Commissioner v. Facebook Ireland Ltd.. (Schrems II)* C-311/18. ECLI:EU:C:2020:559.