International Journal of Law and Information Technology, 2024, **32**, eaae019
https://doi.org/10.1093/ijlit/eaae019
Advance access publication 18 September 2024
Article

Digital identity: an approach to its nature, concept, and functionalities

Margarita Robles-Carrillo[*]

ABSTRACT

Digital identity is a basic component of the knowledge economy and society. It is the key for accessing the digital world and for carrying out commercial, economic, or any kind of transactions and communications. Far from being a merely digital version of the physical identity, digital identity is a singular and complex construct which poses three main dilemmas that provide the framework for its analysis. The first arises from the context in which it is located, the digital ecosystem, that changes its scope and nature. The second, conceptual, is a consequence of the lack of agreement about its definition but also of the different legal framework derived from it. A third dilemma, functional, is due to the fact that digital identity can fulfil different, even contradictory, functionalities. An analysis of these dilemmas can contribute to a better understanding of this category leading to a proposal for its definition and legal framework.

KEYWORDS: digital identity; digital ecosystem; nature; concept; functions**.**

INTRODUCTION

Digital identity is a basic component of the knowledge economy and society. Although its importance did not become evident on a global scale until the health pandemic,[1] for a long time now, digital identity has been the key to have access to the digital world and to carry out commercial, economic, or any kind of transactions and communications.[2] International organisations, at the universal,[3]

[*] Margarita Robles-Carrillo, Full Professor of International and European Law, University of Granada, Spain. Email: mrobles@ugr.es.

[1] Keren Weitzberg *et al.*, 'Between Surveillance and Recognition: Rethinking Digital Identity in Aid' (2021) 8 (1) Big Data & Society 2.

[2] Joseph J. Atick, *Digital Identity: The Essential Guide* (2017) 2, available at https://www.id4africa.com/main/files/Digital_Identity_The_Essential_Guide.pdf; Pat Walshe, *Digital Identities* 3, available at https://rm.coe.int/digital-identity/16809f3ba2; Clare Sullivan, 'Digital Citizenship and the Right to Digital Identity under International Law' (2016) 32 Computer Law & Security Review 481. According to the EU Blockchain Observatory, '(t)here are few things more central to a functioning society and economy than identity. Without a way to identify each other and our possessions we would hardly be able to build large nations or create global markets' (European Union Blockchain Observatory, *Blockchain and Digital Identity* (2019) 8, available at https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf).

[3] In the framework of the United Nations Organization, there are many different agencies working on digital identity. The UNHCR, the Refugee Agency, has adopted several measures including a Strategy on Digital Identity and Inclusion (https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/03/2018-02-Digital-Identity_02.pdf). The United Nations

interregional,[4] and regional levels,[5] legal or technical institutions,[6] alliances,[7] and different agencies[8] are actively working on digital identity. More and more countries worldwide are defining digital identification systems domestically[9] or through international treaties.[10] In the academic field, Sullivan observes that precisely its value as a primary means of accessing networks and services 'is elevating digital identity to an unprecedented level of personal, commercial and legal significance'.[11] Rodrigues

Commission on International Trade Law has approved in 2022 the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services including provisions on this topic (https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mlit_en.pdf). The International Telecommunication Union (ITU) has adopted several recommendations concerning its governance and management, as well as some basic guidelines as the Digital Identity Roadmap Guide (https://www.itu.int/pub/D-STR-DIGITAL.01-2018). In 2022, the World Intellectual Property Organization (WIPO) has presented a White Book about Blockchain technologies and IP ecosystems (https://www.wipo.int/meetings/es/details.jsp?meeting_id=69689) including its digital identity framework. In 2023, the Committee on WIPO Standards has defined a global identifier (https://www.wipo.int/meetings/es/details.jsp?meeting_id=75413). The International Civil Aviation Organization (ICAO) is looking for 'a system of identity and trust that integrates the wisdom of the Chicago Convention into the digital world' (https://www.icao.int/safety/Documents/ICAO_SR_2019_final_web.pdf). The World Bank has been working on digital identity covering different areas such as development through its *Digital Identity Toolkit. A Guide for Stakeholders in Africa* (https://openknowledge.worldbank.org/entities/publication/7e5aa471-da85-531b-a921-a0122ed93e1e) or financial inclusion in its report *G20 Digital Identity Onboarding* (https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf). The World Trade Organization (WTO) has adopted some reports concerning different aspects of this topic (https://www.wto.org/spanish/res_s/booksp_s/tradtechpolicyharddigit0422_s.pdf, 3) as well as measures such as the Standards Toolkit for Cross-border Paperless Trade including provisions on digital identity (https://www.wto.org/english/res_e/publications_e/standtoolkit22_e.htm).

[4] In 2007, the Organization for Economic Cooperation and Development (OECD) presented its report *At a Crossroads: "Personhood" and Digital Identity in the Information Society* (https://one.oecd.org/document/DSTI/DOC(2007)7/en/pdf). It is still actively working on this issue. A Recommendation of the OECD Council on the governance of digital identity was adopted in June 2023 (https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491). In a different context, for instance, the Council of Arab Economic Unity signs in 2020 an agreement with IDEMIA, specialized in the field of digital identity, with the aim of implementing some strategic projects considered vital for Arab countries in order to improve the competitiveness of their economies and their integration into the global economy through digital identity (https://www.idemia.com/news/council-arab-economic-unity-signs-agreement-idemia-security-solutions-2020-08-25?export=pdf&post_id=1445&force).

[5] The European Union has approved Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (https://eur-lex.europa.eu/eli/reg/2024/1183/oj). The Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data of the Council of Europe has adopted in 2023 its *Guidelines on National Digital Identity* (https://edoc.coe.int/en/data-protection/11578-guidelines-on-national-digital-identity.html). There are also several relevant initiatives in Africa: the Digital Transformation Strategy for Africa (2020–2023) considers digital identity in two of its chapters (https://au.int/es/node/38507); Smart Africa Trust (https://sata.smartafrica.org/) and WURI Project are working on some digital identification procedures and platforms (https://www.ecowas.int/wuri-pilot-countries-adopt-governance-framework/); in 2022, the Interoperability Framework for Digital ID was adopted (https://au.int/en/documents/20231211/au-interoperability-framework-digital-id); and, in 2023, the African Digital Identity Landscape offers a global analysis about this question (https://www.uneca.org/sites/default/files/DITE-AFRICA/Africa Digtial ID Landscape Report %282023%29.pdf). The ASEAN has presented in 2021 its Digital Masterplan 2025 including measures about digital identity (https://asean.org/book/asean-digital-masterplan-2025). In 2022, it has created the ASEAN Digital Credentials Platform – AKREDI (https://www.akredicredentials.com/about-us/).

[6] In addition to the Request for Comments on this topic issued by the Internet Engineering Task Force (IETF) (https://www.ietf.org/), the International Organization for Standardization (ISO) has adopted several standards concerning digital identity, particularly, through ISO/IEC 24760 (https://www.iso.org/standard/77582.html). In the World Wide Web Consortium (W3C), there are two groups dedicated to this question: the W3C Digital Identity Community Group and the W3C Decentralized Identifier Working Group (https://www.w3.org/). Open ID Foundation considers its mission to lead the global community in creating identity standards that are secure, interoperable, and privacy-preserving. (https://openid.net/foundation/).

[7] The ID2020 Alliance, for example, has adopted a Manifesto codifying the ethical principles for digital identity (https://www.id2020.org/assets/pdf/ID2020-Alliance-Manifesto.pdf) and has also defined its technical requirements as well as a certification framework (https://www.id2020.org/assets/pdf/ID2020-TAC-Requirements-v1.01.pdf).

[8] There are the cases of Sovrin Foundation (https://sovrin.org/), Hyperledger (https://sovrin.org/library/), IDEMIA (https://www.idemia.com/), or the European Self-Sovereign Identity Framework (https://decentralized-id.com/government/europe/eu/ebsi-essif/).

[9] Estonia has been one of the most advanced countries in this area (https://e-estonia.com/solutions/e-identity/id-card/). The Aadhaar system in India, based on biometric technology, is considered a study case (https://uidai.gov.in/). Australia has developed two systems: Digital Identity y myGov (https://my.gov.au/en/about/help/digital-identity). An increasing number of states are adopting digital identification systems.

[10] Australia (https://www.dfat.gov.au/sites/default/files/australia-singapore-digital-economy-agreement.pdf), the UK (https://assets.publishing.service.gov.uk/media/646356fc94f6df000cf5eaf4/CS_Ukraine_2.2023_UK_Ukraine_Digital_Trade_Agreement.pdf), and Singapore (https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/UKSDEA; https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/KSDPA) are the countries that have concluded most agreements including specific provisions on digital identity.

[11] Clare Sullivan, 'Protecting Digital Identity in the Cloud: Regulating Cross Border Data Disclosure' (2014) 30 Computer Law & Security Review 139; Clare Sullivan, 'Digital Identity and Mistake' (2012) 20 International Journal of Law and Information Technology 224.

states that digital identity is 'a pervasive and dynamic phenomenon of contemporary society with important personal, social, economic and legal ramifications'.[12] It has indeed other significant implications, including philosophical, psychological, sociological, and anthropological ones.

Identity issues permeate human history, as Takemiya and Vanieiev illustrate when they point out that, in the Torah, 'Jacob fakes the identity of his brother in order to get a blessing from his father'.[13] Erich Fromm argues that the need for a sense of identity is so vital and imperative that humans could not be well without finding some way to satisfy it.[14] According to the Commission nationale de l'informatique et des libertés, identity is 'une composante importante de l'organisation de toute société, car elle permet notamment d'attribuer un statut ou un rôle à chacun dans une organisation collective'.[15] Therefore, identity is not simply a word, but a fundamental human trait or component, as well as the basis of individual and social human existence and survival.[16]

Digital identity is consequently both an interdisciplinary and polyhedric category. It has been examined in many disciplines ranging from law, economics, or political science to psychology, sociology, anthropology, or philosophy. Identity is considered a contextual, dynamic, evolutionary, multi-dimensional, variant, and complicated subject.[17] It is also described as 'a mercurial concept the law struggles to regulate'.[18] Digital identity is a complex technical and legal-political category that requires a holistic approach.[19]

There is a growing necessity to address the basic aspects of digital identity from a juridical point of view since international and national authorities, as well as private agencies, academic, industries, companies, and citizens are increasingly concerned about it. Analysing legal and technical regulations, international practice, and academic doctrine, it emerges that digital identity poses three main dilemmas. The first dilemma is *contextual*: it is the result of the different background and landscape provided by the digital ecosystem. The second dilemma is *conceptual*: it arises from the lack of a common definition of digital identity and its legal consequences. The third dilemma is *functional*: it derives from the fact that digital identity may serve different or even contradictory functionalities as can be seen in certain basic areas such as human rights,

[12] Rowena E. Rodrigues, 'Revisiting the Legal Regulation of Digital Identity in the Light of Global Implementation and Local Difference' (2011) (Thesis Doctoral at the University of Edinburgh) 9, available at https://era.ed.ac.uk/handle/1842/8942?show=full.

[13] Makoto Takemiya and Bohdan Vanieiev, 'Sora Identity: Secure, Digital Identity on the Blockchain', IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), (2018) 582–587.

[14] Erich Fromm, *El miedo a la libertad* (Paidós 1980) 278–279.

[15] Commission nationale de l'informatique et des libertés, *L'identité numérique* (2023) 2, available at https://www.cnil.fr/fr/la-cnil-publie-son-premier-dossier-thematique-dedie-lidentite-numerique

[16] Rodrigues, (n 12) 26. See Cristopher Allen, *The Path to Self-Sovereign Identity* (2016) available at https://decentralized-id.com/literature/self-sovereign-identity/.

[17] Rodrigues, (n 12) 27; Andrej J. Zwitter *et al.*, 'Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual' (2020) 3 (26) *Hypothesis and Theory* 3, available at https://www.frontiersin.org/articles/10.3389/fbloc.2020.00026/full. According to Knight and Saxby, digital identity 'combines multi-disciplinary perspectives of psychology, physiology and philosophy, amongst others academic areas. While theories of identity from different disciplines persevere, technological developments, in hand with economic and societal changes, affect modern identity perceptions, its construction and presentation' (Alison Knight and Steve Saxby, 'Identity crisis: Global Challenges of Identity Protection in a Networked World' (2014) 30 Computer Law & Security Review 618.

[18] Umar Mir *et al.*, 'AI-enabled Digital Identity – inputs for stakeholders and policymakers' (2021) 2 Journal of Science and Technology Policy Management 2, avalaible at https://www.emerald.com/insight/content/doi/10.1108/JSTPM-09-2020-0134/full/html?skipTracking=true

[19] Oskar J. Gstrein and Dimitry Kochenov, 'Digital Identity and Distributed Ledger Technology: Paving the Way to a Neo-Feudal Brave New World?' (2020) 3 (10) Hypothesis and Theory 6, available at https://www.frontiersin.org/articles/10.3389/fbloc.2020.00010/full. According to Rasouli et al., 'identities are exposed to a brand-new situation. The digital identity of individuals has been considered as a substructure to provide electronic government (e-government) services. Further, in a modern and advanced information community, it has been regarded for many other electronic services (e-services). Digital identity has transformed human societies and entered them into a new area that needs new and advanced tools for managing it. The usage of digital identity has many privileges in the form of e-government and electronic city (e-city). But it should be considered that the identification and confirmation of digital identity in such spaces are the challenging discussions of today's world. Each concept has accompanied social, legal, economic, and political consequences, which indicate the significance of cyberspace' (Hatef Rasouli *et al.*, 'Proposing a Digital Identity Management Framework: A Mixed-Method Approach' (2021) 33 (2) Concurrency and Computation Practice and Experience 2).

economy, or development. The article ends with some conclusions, proposes a definition, identifies the legal framework, and outlines three of the main issues that still need to be discussed in the context of digital identity.

THE CONTEXTUAL DILEMMA

Digital identity has been conceived as the online version of the physical identity of a person. It is easy and natural to draw parallelisms in the digital sphere, although they are not always real or useful. Much of the common *ethos* of identity has been lost in the digital translation. This process can be illustrated by attending to its *context*—which is quite different from the previous one—and to the *distinct nature* of digital identity.

A different context

There are several factors that explain the paradigmatic change in the idea of identity in the digital scenario. Both the understanding and functionality of identity are different in this context.

Firstly, in the digital world—commonly defined as the realm of anonymity—any subject can have at the same time several, different, real, imaginary, or false identities. This is a fundamental difference from the natural domain where physical and legal identities are a unique and exclusive quality. By contrast, in the virtual space, there might be multiple and diverse identities associated with the same user and with the same status. As a result, the processes of identity accreditation and authentication are more complex, more vulnerable, and less reliable. The emergence of specific virtual worlds such as the metaverse increases and additionally complicates the situation because it implies more and more different scenarios for digital identity users.[20]

Secondly, in contrast with the previous situation—where legal identity is not always needed, recognized, or wanted, in the case of countries where it is not part of the legal system—the lack of a secure and reliable digital identity limits and prevents access to digital economy and society. It can even restrict the exercise of basic rights such as the freedom of expression or the right to information. Actually, digital identity raises several issues in the field of human rights: not only whether it is an autonomous human right or a provider of basic rights, but also whether some identification techniques can lead to a violation of human rights.

Thirdly, contrary to the physical world—where it is recognized as a public function of states—the main providers of digital identity are non-state actors operating on a transnational level.[21]There is not one universal or uniform system of digital identification, which would be ideal

[20] Irina A. Filipova, 'Creating the Metaverse: Consequences for Economy, Society, and Law' (2023) 1 Journal of Digital Technologies and Law 7; Ana M. Martín Elvira, 'El metaverso: potenciales riesgos y amenazas para la paz y la seguridad, y su contagio en el mundo real' (2023) 40 Boletín IEEE 7; Fabiana Di Porto and Daniel Foà, *Defining Virtual Worlds: Main Features and Challenges*, Centre on Regulation in Europe, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4507397.

[21] Florence G'sell and Florian Martin-Bariteau, *The Impact of Blockchains for Human Rights, Democracy, and the Rule of Law* (2022) 23, available at https://rm.coe.int/report-on-blockchains-en/1680a8ffc0). Sam Altman, CEO of the OpenAI, has announced the Worldcoin project with the goal of creating a new digital identity and financial network accessible to everyone online. The World ID allows individuals to prove their uniqueness online. It consists of a digital identity called World ID, and a digital currency called WLD (https://dig.watch/updates/digital-identity-network-worldcoin-created-by-the-openai-ceo-sam-altman). Haimson and Hoffmann identify some of the issues arising from digital identification through private companies. According to the authors, 'given its size and influence online, Facebook has worked to impose an administrative notion of authenticity on a large portion of the world's population. This administrative conception of identity is captured in Zuckerberg's discourse surrounding authenticity, identity, and the directory-oriented nature of Facebook's foundations. Facebook's view of authenticity is also reflected in its mechanisms for enforcing "authentic identity" through site policy and design, as demonstrated in our analysis of site walkthroughs. Ultimately, the combination of discourse and design generates conditions that exclude or make online life disproportionately difficult for certain groups, including trans people, abuse survivors, and Native Americans. By defining and challenging Facebook's construction and enforcement of authenticity, we encourage considerations of how discourse and design could be approached differently, to allow all users to be as authentic or inauthentic as they choose, no matter how fluid, contextual, and socially constructed that identity may be' (Oliver L. Haimson and Anna L. Hoffmann, A.L., *Constructing and Enforcing "Authentic" Identity Online: Facebook, Real Names, and Non-Normative Identities* (2022), available at https://firstmonday.org/ojs/index.php/fm/article/view/6791/5521).

in a global community such as digital space.[22] Therefore, digital identity solutions are mostly private, heterogeneous, and fragmented depending on different providers and services.[23] In addition, digital identity is being managed for economic and commercial purposes.[24] Accessing a provider or a service implies accepting its digital identification system. There is usually no choice and there are not always guarantees of respect for basic rights such as privacy or data protection in the identification process. User identity data is now a commodity while human identity becomes part of the technological structure.[25] Private corporations' power over identity is actually a much deeper problem.[26] Benvenisti has identified the problem derived from the privatization and monopolization of the communicative space, while De Gregorio and Radu had warned about fragmentation, polarization, and hybridization in the governance of digital technologies.[27]

Fourthly, the virtual world requires objects and devices, as well as people, to have an identity. According to Priem *et al.*, 'historically, device identity preceded human identity in the online environment because the internet was developed as a computer-to-computer infrastructure'.[28] As Friedman y Wagoner state, 'an IT system is a closely connected group of interconnected elements that all require digital identity … an IT system is composed of five parts: people, procedures, software, hardware, and data. There are unique challenges and different identity techniques that are emerging to create digital identity within each category'.[29] Any one component requires a separate identity, because of its own nature and features, but all of them must be compatible in order to allow interconnection.

Fifthly, a secure identity is the cornerstone of any cybersecurity model.[30] The weakest and most vulnerable layer within this system are generally users. Far from being a merely theoretical concept, digital identity is of great practical importance. The current situation poses two main problems: on the one hand, it forces individuals to use various usernames and passwords and to rely on different providers accessing and using their data; and on the other hand, it compels

[22] In this regard, Goodell y Aste explain that 'the search for unitary identities for individual persons is problematic. It is technically problematic because there is no endogenous way to ensure that an individual has only one self-certifying name, there is no way to be sure about the trustworthiness or universality of an assigned name, and there is no way to ensure that an individual exists only within one specific community. More importantly, we assert that the ability to manage one's identities in a multitude of different contexts, including the creation of multiple unrelated identities, is an essential human right' (Geoff Goodell and Tomaso Aste, 'A Decentralized Digital Identity Architecture' (2019) 2 Front Blockchain 2, available at https://www.frontiersin.org/articles/10.3389/fbloc.2019.00017/full).

[23] European Union Blockchain Observatory (n 2) 8. Examples of public and private usage of digital identity and their evolution can be found in Commission nationale de l'informatique et des libertés (n 15) 6.

[24] Rachel Griffin, 'Public and Private Power in Social Media Governance: Multistakeholderism, the Rule of Law and Democratic Accountability' (2022) 14 (1) Transnational Legal Theory 24.

[25] Arthur R. Friedman and Larry D. Wagoner, 'The Need for Digital Identity in Cyberspace Operations' (2015) 14 (2) Journal of Information Warfare 42–43; Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data of the Council of Europe, *Guidelines on National Digital Identity* (2023) 6, available at https://edoc.coe.int/en/data-protection/11578-guidelines-on-national-digital-identity.html.

[26] To the extent that the state is the locus of democratic accountability, as Griffin points out, it is necessary to focus the analysis on the 'public foundations of private power' (Griffin (n 24) 24).

[27] According to Benvenisti, 'whereas governments in the past have traditionally invested in the gathering and management of information as a way to ensure compliance with the law and to plan ahead, they are nowadays increasingly dependent on a handful of private ICT companies that regard the services they provide and the data that they amass as their private property and subject to their own discretion. Voters, in turn, are relegated to the role of users, whose rights are determined by non-negotiable boilerplate service agreements and whose bounded rationality is closely studied and exploited by the service providers. These companies invoke their private status and their right to exclusive use of their data and their algorithms as grounds to remain unaccountable and otherwise unencumbered by the discipline of public law' (Eyal Benvenisti, 'Upholding Democracy Amid the Challenges of New Technology: What Role for the Law of Global Governance?' (2018) 29 (1) The European Journal of International Law 71); Giovanni De Gregorio and Roxana Radu, 'Digital constitutionalism in the new era of Internet governance' (2022) 30 (1) International Journal of Law and Information Technology 68–87.

[28] Bart Priem *et al.*, 'The Identity Landscape', in J. Camenisch *et at.*, (eds.), *Digital Privacy. PRIME – Privacy and Identity Management for Europe* (2011) 33. In the case of AI devices, see Abdulrahman S. S. Aldossary, 'Digital IDs for advanced robotics systems as a regulatory infrastructure,' (2022) 30 (3) International Journal of Law and Information Technology 350–367.

[29] Friedman and Wagoner (n 25) 42–43.

[30] White House, *National Strategy for Trusted Identities in Cyberspace. Enhancing Online Choice, Efficiency, Security, and Privacy* (2011) 1–2, available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

authorities, institutions, and companies to increase identification services and costs. Neither governments nor private providers can effectively guarantee the security and reliability of every identification process.[31]

Finally, but no less important, any digital identity model has to be an interplay of technical and legal aspects. However, the relationship between law and technology is far from being straightforward.[32] Two different types of problems may arise: firstly, whether a legal requirement cannot be technically implemented and secondly, whether a technical device does not meet or cannot comply with the regulatory framework. In the latter case, it is not legal. In the former, the normative might be ineffective or useless. A careful understanding of both technical and legal aspects is required for every digital identity solution. Accepting this fact, however, it should be noted that it is leading in practice and even in the development of the regulatory processes themselves to a situation to which attention should be drawn. Technical institutions, standardization organizations, and various actors, that are not subject to the requirements of public entities, are designing the technical standards not only to develop digital identity management models, but also to define the concept itself and determine its functionalities. To the extent that countries and international organizations rely on such work in order to design regulatory frameworks for digital identity, the need for better clarification of the scope of their respective roles should be considered. In the context of the necessary public–private cooperation, a rethink is needed on how and when to integrate technical requirements into regulatory processes. As this article attempts to explain, both the concept and the functionalities of digital identity raise issues of particular legal-political significance that require an in-depth reflection that cannot be relied upon the so-called technological solutionism.

To sum up, in the digital field, identity is something different, more complex, and challenging than the traditional one. It has to face several problems, mainly: the extreme fragmentation of the digital identity landscape; the goal of ensuring general access to digital space; the privatization of this function; the need to distinguish and coordinate identity procedures for humans, devices, and processes; the request for secure and reliable methodologies; and the setting-up of both technical and legal requirements.[33] According to Knight and Saxby, the problems raised in this field seem to be leading to a global identity crisis.[34]

A different category

Digital identity is not the digital twin of identity. An analysis of academic doctrine and international practice reveals their main differences.[35] Firstly, the uniqueness and singularity of identity in the physical world are in clear contrast with the variety of identities commonly used in the

[31] As Aresty observes, 'in comparison to the physical world, in which one's identity is readily verifiable through the application of senses, in the digital realm, it is difficult to verify identity. (…) Digital communications are prone to misinterpretation, and because digital communications are characterized by anonymity, accountability is virtually nonexistent. (…) It is both easy and common to change one's online identity' (Jeffrey Aresty, 'Digital identity and the Lawyer's Role in Furthering Trusted Online Communities' (2006) 38 (1) University of Toledo Law Review 143).

[32] Tatar et al. argue that 'inconsistency between the way in which the law is structured, and the way in which technologies actually operate is always an interesting and useful topic to explore. When a law conflicts with a business model, the solution will often be changing the business model. However, when the law comes into conflict with the architecture of hardware and software, it is less clear how the problem will be managed' (Unal Tatar *et al.*, 'Law versus Technology: Blockchain, GDPR, and Tough Tradeoffs' (2020) 38 (1) Computer Law & Security Review 105454).

[33] In some common law countries, there are some additional problems insofar as identity has not traditionally been recognized as a legal category (Sullivan, *Protecting,* (n 11) 139; A. Boothe, 'The death and life of Jang Nayeon: a case for personality rights in the digital layers of reality' (2022) 30 (4) International Journal of Law and Information Technology 398–422). There are cases, such as the UK, where identity cards don't exist as well as others, such as some African countries, where there have no means of attributing this legal status. In the digital field, the situation is totally different. The UK has created the Office of Digital Identities and Attributes as part of an overall plan to establish trusted and secure digital identities (https://www.gov.uk/government/news/new-legislation-set-to-make-digital-identities-more-trustworthy-and-secure). Many African or American countries are turning to digital identity to overcome the problem of their legal identity gap (https://au.int/Agenda2063/popular_version).

[34] Knight and Saxby (n 17) 629.

[35] Rodrigues (n 12) 29 and 60–62.

virtual world.[36] Following Aresty and Church, there are many legitimate reasons for simultaneously maintaining more than one-identity online,[37] although it should also be recognized that multiple identities are also kept with malicious or negative intentions.[38] Secondly, as a result of this situation, as Saxby, Lyons, and Soltani *et al.* point out, there is a weak link or even a real divorce between physical and digital identities.[39] Thirdly, even if identity was already a complex concept in the physical environment, in the online world, according to Priem *et al.*, 'it is even a more "muddled thing" because the Internet provides the possibility of disembodied use of identities and facilitates the decontextualization and transfer of identities'.[40] Fourthly, as Lyons *et al.* argue, digital identity is not a single thing 'but rather the sum total of all the attributes that exist about us in the digital realm—a constantly growing and evolving collection of data points'.[41] Finally, Zwitter *et al.* explain that 'whereas traditionally identity is addressed in a predominantly sectoral fashion whenever necessary, new technologies transform digital identity management into a basic infrastructural service, sometimes even a commodity'.[42]

Acknowledging those differences between physical and digital identity, Knight and Saxby have advocated for a different conception of this category following a less static and more dynamic paradigm in which identity is 'doing in addition to being'.[43] Although law has traditionally conceived the citizen as having a single, panoptic identity to which rights and responsibilities are attached, in their opinion, 'the conception of a fixed, single identity becomes a legal fiction' because of 'the changing nature of online identity'.[44] Greenwood proposes a typology that distinguishes between digital identity, physical identity, and dual or convergent identity that would result from the combination of the above.[45] Finally, Sullivan argues in favour of maintaining the one-person-one-identity premise. Whereas in the private sphere, this may be different, in the public domain it is essential since a governance model requires uniqueness and exclusivity.[46]

In the light of these points, differences between physical and digital identities seem clear. In addition, to the extent that a single, tangible, physical identity can encompass distinct digital identities, another challenge is to organize the relationship between them both legally and technically. By 2007, UNESCO had already proposed that a unique digital legal identity might be a solution.[47] However,

[36] Zhao *et al.* explain that 'the presence of the corporal body in social encounters prevents people from claiming identities that are inconsistent with the visible part of their physical characteristics, and the shared knowledge of each other's social background and personality attributes renders it difficult for an individual to pretend to be what he or she is not. (…) The advent of the Internet has changed the traditional conditions of identity production (…) The combination of disembodiment and anonymity creates a technologically mediated environment in which a new mode of identity production emerges. (…) An important characteristic of this emergent mode of identity production is the tendency for people to play-act at being someone else or to put on different online personae that differ from their "real life" identities … In other words, the disembodied and anonymous online environment makes it possible for people to reinvent themselves through the production of new identities' (Shanyang Zhao *et al.*, 'Identity Construction on Facebook: Digital Empowerment in Anchored Relationships' (2008) 24 (5) Computers in Human Behavior 1817–1818, available at https://www.sciencedirect.com/science/article/abs/pii/S0747563208000204).

[37] Aresty (n 31) 144. According to Church, 'we can choose our digital identity. We can construct different identities or choose to only show some of ourselves to certain audiences. We can engage with others under pseudonyms providing anonymity or we can share all our thoughts and beliefs under our real identity' (Carey Church, 'Your Digital Identity and Assets Are Important. So What Can You Do To Protect Them?' (2015) 23 Waikato Law Review 151).

[38] Aresty (n 31) 144.

[39] Tom Lyons *et al.*, *Blockchain and Digital Identity*, 2019, 9, available at https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf; Steve Saxby, 'The 2013 CLSR-LSPI Seminar on Electronic Identity: The Global Challenge' (2014) 30 (2) Computer Law & Security Review 112–125; Reza Soltani *et al.*, 'A Survey of Self-Sovereign Identity Ecosystem' (2021) Security and Communication Networks 8873429, 4, available at https://www.hindawi.com/journals/scn/2021/8873429/.

[40] Priem *et al.* (n 28) 35.

[41] Lyons, Courcelas and Timsit (n 39) 5.

[42] Zwitter *et al.* (n 17) 6.

[43] Knight and Saxby (n 17) 629.

[44] ibid 618–619.

[45] Daniel Greenwood, *Context for Identity Management Architectures and Trust Models* (2007), paper presented at the OECD Workshop on Digital Identity Management, Trondheim, 5.

[46] Sullivan, *Protecting* (n 11) 139.

[47] UNESCO, *Ethical Implications of Emerging Technologies* (2007) 38, available at https://unesdoc.unesco.org/ark:/48223/pf0000149992

the plurality and diversity of digital identity models supported by countries and providers make it difficult to reach a single system or to develop a uniform model regarding the relationship between physical and digital identities. For now, the debate is raging between those who advocate transferring the uniqueness of physical identity to the digital field and those who do not accept constraining the digital sphere by the parameters of the physical domain. This is the dilemma imposed by the context: not only does it change the category, but it also raises the need to articulate its relationship with its physical counterpart from which it comes but to which it is clearly different. Complicating matters is the fact that, in addition to the absence of a single model of digital identity, there is no common definition of this concept.

THE CONCEPTUAL DILEMMA

There is not one single or general definition of digital identity.[48] Although it has been easily and hastily conceived as the online version of physical identity, it is a broad and more complex concept mainly for three reasons. Firstly, as has been seen, there are significant differences between digital and physical identity. Secondly, even if it is not considered a substantive right, digital identity is the instrumental right that enables access to the digital world. Thirdly, it performs three basic technical functions: identification, authentication, and authorization. Digital identity has unique *features* that might justify the lack of consensus concerning its *definition* which can explain to the conceptual dilemma.

Conceptual features

The most distinctive property of digital identity is that it is a universal concept able to serve different functions in different contexts. Atick, Priem *et al.,* Knight and Saxby highlight that it is a concept shaped by contexts and circumstances.[49] As a second main feature, digital identity is a dynamic and multifaceted category with several dimensions and functions. According to Priem *et al.*, it is used to represent a person and to identify and recognize such a person 'both in descriptive terms and process terms'.[50] For that reason, the authors distinguish between the so-called *ipse* identity referring to who a person is, and the *idem* identity relating to how a person is characterized or represented by himself or by others. A third outstanding trait is that digital identity is a fragmented, layered, composed, and changing concept.[51] It is a very complicated category with many levels ranging from the philosophical to the practical.[52]

According to the OECD, digital identity is both a 'real world concept and a digital artifact'.[53] Lyons *et al.* consider that it is atomic in nature as being based on discrete bits of information as well as cumulative. As a result, it is not a single thing but 'the sum total of all the attributes that exist about us in the digital realm, a constantly growing and evolving collection of data points'.[54] Moreover, digital identity can be built on different types of attributes. Church identifies the basic three: inherent, acquired, and individual characteristics.[55]

[48] Walshe (n 2) 2.

[49] Knight and Saxby (n 17) 618; Priem *et al.* (n 28) 34. Atick argues that digital identity is a critical concept in the digital society which has the particularity of being a universal category that nevertheless serves different functions in different countries and contexts. It can be 'game changer and poverty killer' (Atick, (n 2) 3).

[50] Priem *et al.* (n 28) 34.

[51] Rodrigues (n 12) 6–7.

[52] Joseph Pato, 'Identity Management: Setting Context. Technical Reports' (2003) Encyclopedia of Information Security 1, available at https://zoo.cs.yale.edu/classes/cs155/spr03/idmgmt-tr.pdf.

[53] OECD, *At a Crossroads: "Personhood" and Digital Identity in the Information Society* (2007) 26, available at https://one.oecd.org/document/DSTI/DOC(2007)7/en/pdf

[54] Lyons *et al.* (n 39) 12.

[55] Church (n 37) 152.

As early as 2007, the OECD has already identified the following properties of digital identity: social, subjective, valued, referential, composite, consequential, dynamic, contextual, and ambiguous. Rodrigues considers that it can be unitary or multiple, equal or different, fixed or flexible, local or universal, authentic or fictitious, possessed or owned, assigned or assumed, fragmented or cohesive, public or private, anonymous or pseudo-anonymous, temporary or permanent, and visible or invisible.[56] According to the National Institute of Standards and Technology, the main features of digital identity are security, privacy, equity, and usability.[57]

In light of these features and properties, digital identity is clearly different from physical identity and is a concept difficult to define because of its own nature and characters and because of these dissimilarities with its predecessor in the physical world.

Conceptual proposals

The concept of digital identity has become the focus of much and in-depth discussion.[58] As Lips notes, even if the term identity management has been widely used both in practice and in the academic field, 'a commonly accepted meaning for the term is lacking so far'.[59] After reviewing the different approaches followed by international organizations and institutions, Mir *et al.* point out that it is a very complex notion with multiple dimensions that has been the subject of a wide variety of proposals without reaching a consensus.[60] By 2008, Lips had already systematized the main conceptual proposals.[61] Shibuya offers a survey of the definitions provided in philosophical and semantic studies, among others.[62] Soltani *et al.* consider that those definitions are mostly inconsistent while, in their view, 'a definition founded on mathematical properties would help in providing a uniform definition of digital identity and reduce confusion'.[63] As can be seen, across and within the different areas of knowledge, the conceptual debate is deep, complicated, and not limited to the academic level.

This crack in the conceptual debate is well known in the academic domain, where it is a normal and constructive part of the discussion. However, it is a phenomenon that is emerging as well in the regulatory area and even within the same legal system, something that is neither normal nor secure nor constructive. As Friedman and Wagoner explain, in the US Administration, digital identity has been defined simultaneously in three different ways. It is 'the representation of identity in a digital environment'. It is 'a set of attributes that represent a subject in an online transaction'. And it is 'the digital representation of a set of claims made by one digital subject about itself or another digital subject'.[64] Although they appear to be similar, they are not the same in legal terms. A second example in this regard is provided by the OECD. In 2007, digital identity was defined as 'a digital representation of a set of claims made by one party about itself or another data subject'.[65] In 2023, digital identity refers to 'a set of electronically captured and stored attributes and/or credentials that can be used to prove a quality, characteristic, or assertion about a user, and, when required, support the unique identification of that user'.[66] Finally,

[56] OECD, *At a Crossroads* (n 53) 7.

[57] National Institute of Standards and Technology, *Digital Identity Guidelines* (2023) 6–9, available at https://doi.org/10.6028/NIST.SP.800-63-4.ipd

[58] Aresty (n 31) 141–142.

[59] Anna Lips, *Identity Management in Information Age Government. Exploring Concepts, Definitions, Approaches and Solutions.* (2008) 3, available at https://www.researchgate.net/publication/259972539_Digital_Identity_Management

[60] Mir *et al.* (n 18) 2.

[61] Lips (n 59) 3.

[62] Kazuhiko Shibuya, *Digital Transformation of Identity in the Age of Artificial Intelligence* (2020) 25, available at https://doi.org/10.1007/978-981-15-2248-2_2

[63] Soltani *et al.* (n 39) 4.

[64] Friedman and Wagoner (n 25) 41.

[65] OECD, *At a Crossroads* (n 53) 7.

[66] OECD, *Recommendation of the OECD Council on the Governance of Digital Identity* (2023) 6, available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491.

a third case is offered by ENISA. In the same report and on the same page, digital identity is defined as 'a unique representation of a subject engaged in an online transaction' and, also, as 'a set of attributes related to an entity'.[67] A 'representation', 'a set of attributes', or a 'representation of a set of attributes' are not ontologically the same thing. They cannot be conceptually interchangeable to define the same entity. In legal terms, it is essential to be much clearer and much more precise.

An analysis of institutional and academic practice reveals that there are five main approaches to this concept. Firstly, digital identity is conceptualized around the idea of representation.[68] Rodrigues states that it is 'the digital representation of a digital identity subject in tangible or intangible form, self-created, externally assigned or consequentially generated'.[69] Fernández Burgueño considers that it is the electronic expression of the set of features with which a person, whether natural or legal, is individualized in relation to others.[70] Following the National Institute of Standards and Technology, digital identity is the unique representation of a subject participating in an online transaction.[71] For ENISA, it is 'the unique representation of a subject engaged in an online registration transaction'.[72]

Secondly, there is a broad academic and technical sector that conceives digital identity as information or as a sum of data, assertions, or attributes. According to Pato, it is the set of information known about a person.[73] For Sule *et al.,* it is a set of individual information or attributes that describe an entity and that is used to determine the transactions in which the entity can legitimately engage.[74] Sullivan as well as the Boston Consulting Group consider that it is the sum of all digitally available information about an individual, regardless of its degree of validity, its form, or its accessibility.[75] Following the ISO/IEC 24760-1, digital identity is 'an item inside or outside an information and communication technology system, such as a person, an organization, a device, a subsystem, or a group of such items that has a recognizably distinct existence'.[76] Friedman and Wagoner consider that it is 'a set of data that uniquely describes a person or thing and contains information about the subject's relationships to other entities'.[77] Beduschi argues that digital identity as a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions.[78] Cameron asserts that it is a set of assertions made by a digital subject about itself or, in this case, also about another digital subject.[79] According to the International Bar Association, digital identity 'is intended to cover the broad set of information encompassed in the definition of identity'.[80] In the Guidelines issued by

[67] ENISA, *Digital Identity Standards. Analysis of Standardization Requirements in Support of Cybersecurity Policy* (2023) 5, available at https://www.enisa.europa.eu/publications/digital-identity-standards

[68] Shibuya (n 62) 2.

[69] Rodrigues (n 12) 9.

[70] Pablo Fernández Burgueño, *Aspectos jurídicos de la identidad digital y la reputación online* (2012) 127, available at http://repositori.uji.es/xmlui/handle/10234/43024

[71] National Institute of Standards and Technology (n 57) 3.

[72] ENISA, *DNS Identity. Verification and Authentication of Domain Name Owners* (2023) 7, available at https://www.enisa.europa.eu/publications/dns-identity

[73] Pato (n 52) 1.

[74] Mary-Jane Sule *et al.*, 'Cybersecurity through the Lens of Digital Identity and Data Protection: Issues and Trends' (2021) 67 Technology and Society (2021) 101734, 2.

[75] Sullivan, *Digital identity and mistake* (n 11) 240; Sullivan, *Protecting, supra* note 11, at 139; Boston Consulting Group, *The Value of our Digital identity* (2012) 20, available at https://www.bcg.com/publications/2012/digital-economy-consumer-insight-value-of-our-digital-identity

[76] https://www.iso.org/standard/77582.html

[77] Friedman and Wagoner (n 25) 41.

[78] Ana Beduschi, 'Rethinking Digital Identity for Post-COVID-19 Societies: Data Privacy and Human Rights Considerations' (2021) 3 Data & Policy 2.

[79] Kim Cameron, *The Laws of Identity* (2005) 6, available at https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

[80] International Bar Association, *Digital Identity: Principles on Collection and Use of Information* (2016) 11, available at https://www.ibanet.org/MediaHandler?id=2E931F85-C5D0-4952-A6E6-6EA48C593155

the Consultative Committee of the 108 Convention of the Council of Europe, it is 'the processing of attributes about an individual so that the individual is uniquely identifiable in given contexts'.[81]

Thirdly, there are also some definitions linking the two previous options. In 2008, the OECD conceived digital identity as 'a digital representation of a set of claims made by one party about itself or another data subject'.[82] For the International Telecommunication Union (ITU), it is 'the digital representation of the information known about a specific individual, group or organization'.[83]

Fourthly, with a different view, Zwitter *et al.* define digital identity as 'a mixture of individual determination and relational aspects'.[84] De Hert considers that it is 'a mix of ipse identity and idem identity. Ipse (or self) identity is the irreducible sense of self of a human person. It is reflexive consciousness of oneself. Idem (or sameness) identity is the objectification of the self that stems from comparative categorization'.[85] In the World Economic Forum, it is 'a collection of individual attributes that describe an entity and determine the transactions in which that entity can participate'.[86]

Finally, there are those who consider that none of these definitions adequately capture the general sense of the term digital identity. This is the conclusion of Friedmann and Wagoner or Rodrigues.[87] Arguments might be different. Following the International Bar Association, for instance, the existing definitions are not appropriate since, being a global issue, it requires a global approach.[88] According to the ITU, the concept of digital identity encompasses a myriad of aspects related to governance, policy, operations, technology, and legality that demand a more comprehensive understanding.[89]

Furthermore, although they may appear similar, definitions based on the idea of representation or on the idea of data or information have very different consequences in legal terms. In the case of the latter, an identity-related incident would involve personal data or non-personal data, depending on whether it is a subject or an object and what kind of object. If digital identity is information or data and corresponds to a person, the data are to be personal. If it corresponds to an object, the data could also become personal if it can be linked to a person. In these cases, digital identity would be covered by the basic right to the protection of personal data. Digital identity conceived as a representation would not have such consequences. Moreover, the idea of representation does not have a clear legal meaning.

At this point, there is no consensus either on the concept or on the model of digital identity even though both are fundamental to the development of the digital economy and society.[90] The conceptual dilemma is not just due to the lack of agreement on the concept or the existence of different proposals about it. It is also caused by the fact that the choice of one or the other implies quite different legal frameworks for this category: to be or not be protected as a right depending on whether or not it involves personal data. This is part of the functional dilemma posed by digital identity.

[81] Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data of the Council of Europe (n 25) 35.

[82] OECD, *At a Crossroads* (n 53) 7.

[83] International Telecommunications Union, *Baseline Identity Management Terms and Definitions* (2010) 3, available at https://www.itu.int/SG-CP/example_docs/ITU-T-REC/ITU-T-REC_E.pdf

[84] Zwitter *et al.* (n 17) 6.

[85] Paul De Hert, *A Right to Identity to Face the Internet of Things* (2007) 15–16, available at https://researchportal.vub.be/en/publications/a-right-to-identity-to-face-the-internet-of-things-2

[86] World Economic Forum, *A Blueprint for Digital Identity. The Role of Financial Institutions in Building Digital Identity* (2016) 5, available at https://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

[87] Friedman and Wagoner (n 25) 29 and 60–62.

[88] International Bar Association (n 80) 11.

[89] International Telecommunications Union, *Digital Identity Roadmap Guide. Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO)* (2018), available at https://www.itu.int/en/ITU-D/ICT-Applications/Documents/Guides/Digital_Identity_Roadmap_Guide-2018-E.pdf. See N. Sundberg, *Digital identity in the ICT ecosystem: An overview* (2018) 3, available at https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.ID01-2018-PDF-E.pdf

[90] Thomas J. Smedinghoff, 'Solving the Legal Challenges of Trustworthy Online Identity' (2012) 28 (5) Computer Law & Security Review 533.

THE FUNCTIONAL DILEMMA

Since identity plays a central role in logics and metaphysics, existentialism, and other areas, Zwitter *et al.* have identified a basic dilemma between two positions: the naturalist view which considers identity as a whole and the constructivist one according to which identity is shared and compartmentalized.[91] In addition to it, in the legal framework and in specific branches of International Law, digital identity raises functional dilemmas. Not all the areas have the same problem.

The core nature and value of identity are generally cyphered in terms of security. According to Manby, many governments highlight 'the primary importance of national security and border control in implementing the new identification systems'.[92] Friedman and Wagoner point out the need for more secure digital identities because of the fact that identity theft has become an exponentially growing criminal activity.[93] The struggle against criminality associated with digital identity has caught the attention of both international and national institutions.[94] Whereas there is consensus on its value from the point of view of security, there is no agreement about its functions in other fields where digital identity can develop different and even opposite functionalities. *Human rights* and *economy and development* are basic areas that might illustrate the functionnal dilemma of digital identity.

Digital identity and human rights

The relationship between digital identity and human rights involves several issues. It is far from being fully and definitely settled. To begin with, as Masiero and Bailur observe, digital identity itself implies the conversion of human identities into machine-readable digital data and so into a part of the digital machinery.[95] It is an evident paradigmatic change. However, human identity should neither be reduced to its expression in technical terms, nor be assimilated to other types of digital identities, not even for technological requirements. Although the implications of this substantive debate are far-reaching, the three specific questions considered below are dominating the discussion about digital identity and human rights.

Digital identity: an autonomous right?

Article 8 of the Convention on the Rights of the Child establishes a right to identity. However, no other legally binding text formally and expressly recognizes this right in general terms. In the absence of a specific legal basis, there are different interpretations as to whether or not it is a right and, if so, its legal foundation. According to the Consultative Committee of the 108 Convention of the Council of Europe, the concept of legal identity has been developed from Article 6 of the Universal Declaration of Human Rights which states that everyone has the right to recognition everywhere as a person before the law.[96] Legal identity is conceived as a right in the report Our Common Agenda of the Secretary General of the United Nations.[97] Providing legal identity for all is the 16.9 goal of the UN 2030 Sustainable Development Strategy.[98] The Special Envoy of the Secretary General for Technology includes digital identity within digital

[91] Zwitter *et al* (n 17) 3.

[92] Bronwen Manby, 'The Sustainable Development Goals and 'Legal Identity for All': First, Do No Harm' (2021) 139 World Development 105343 5.

[93] Friedman and Wagoner (n 25) 42.

[94] Lucy Cradduck and Adrian Mccullagh, 'Identifying the Identity Thief: Is it time for a (smart) Australia Card?' (2008) 16 (2) International Journal of Law and Information Technology, 125–158; ENISA, *Identity Theft* (2020) available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-identity-theft

[95] Silvia Masiero and Savita Bailur, 'Digital Identity for Development: The Quest for Justice and a Research Agenda' (2021) 27 (1) Information Technology for Development 1.

[96] Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data of the Council of Europe (n 25) 6.

[97] https://www.un.org/en/un75/common-agenda

[98] https://sdgs.un.org/2030agenda

rights.[99] Although it is a non-binding text, the Spanish Charter of Digital Rights recognizes the right to identity in the digital environment.[100]

The academic community has been supporting identity as a human right through different arguments.[101] Firstly, some authors base this right on certain treaties, without specifying particular provisions. Among them, Manby states that it is 'a right long-established in the international human rights regime' according to the 1948 Universal Declaration of Human Rights, the 1966 International Covenant on Civil and Political Rights, and a range of other international human rights treaties.[102] Walshe argues that it is founded on the interpretation of human rights instruments, particularly, the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.[103] Secondly, some authors ground this right directly on a specific provision, but not always the same. Aresty locates the legal basis of the right to identity in Article 16 of the International Covenant on Civil and Political Rights.[104] Szreter defends that this right is clearly established in the second clause of Article 24 of the same treaty.[105] De Hert conceives such a right as a consequence of the right to human dignity.[106] Finally, there are other authors who have evolved and changed the foundations of this right.[107]

As can be seen, there is neither consensus about its nature nor on its foundation as a human right. De Hert argues that a specific right to identity should be clearly distinguished from the classical or first-generation rights since digital identity needs to be understood in dynamic terms.[108] Whether or not qualified as a basic right, digital identity is considered an enabler of rights as it provides access to and makes possible the exercise of other rights.[109]

Digital identity: a provider of rights

Digital identity is a requisite for the exercise of some basic rights, notably access to Internet and freedoms of information and expression.[110] As Hannah Arendt explains, the right to have rights is a 'pre-legal premise' or a 'proto-right'.[111] According to the OECD, 'the right to effective digital personhood will arguably be the most fundamental right in the future information society, as it will determine the possibility of a person to enjoy all other rights including civil, political, economic, social, and cultural rights'.[112] Banihashemi[113] and Manby support this argument about

[99] https://www.un.org/techenvoy/es/content/digital-human-rights

[100] https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

[101] Marcela L. López Serna and Julio C. Kala, 'Derecho a la identidad digital, como resultado del libre desarrollo de la personalidad' (2018) 7 (14) Ciencia Jurídica 68–76.

[102] Manby (n 92) 2.

[103] Walshe (n 2) 3.

[104] Aresty (n 31) 141–142.

[105] Simon Szreter, 'The Right of Registration: Development, Identity Registration, and Social Security—A Historical Perspective' (2007) 35 (1) World Development 68.

[106] De Hert (n 85) 16.

[107] In 2011, Sullivan argued that it derives from individual autonomy (Clare Sullivan, *Digital Identity*, (University of Adelaide Press South, 2011) 84). Since 2016, she found its basis in the Convention on the Rights of the Child, as well as in Art. 1 of the International Covenant on Civil and Political Rights and Art. 8 of the European Convention on Human Rights (Sullivan, *Digital citizenship* (n 2) 479–480; Clare Sullivan, 'Digital identity – From Emergent Legal Concept to New Reality' (2018) 34 Computer Law & Security Review 730).

[108] De Hert (n 85) 8–9 and 15.

[109] Kate Hamming, 'A Dangerous Inheritance: A Child's Digital Identity¨ (2020) 43 Seattle University Law Review 1043–1044; López Serna and Kala (n 101) 65–76.

[110] Walshe (n 2) 2.

[111] Hanna Arendt, *The Origins of Totalitarianism* (Meridian Books 1967) 127.

[112] OECD, *At a Crossroads* (n 53) 27.

[113] According to Banihashemi, 'Internet may once have been a nice-to-have amenity. However, as societies have become more dependent on digital infrastructure to conduct and support communication, commerce, culture, and even life-saving emergency services and healthcare, the internet has become a prerequisite to access fundamental human rights' (Pegah Banihashemi, 'International Law and the Right to Global Internet Access: Exploring Internet Access as a Human Right Through the Lens of Iran's Women-Life-Freedom Movement' (2023) 24 (1) Chicago Journal of International Law 34).

digital identity as a way of accessing rights, goods, and services.[114] The same view is shared by Szreter,[115] Aresty,[116] Sullivan,[117] as well as Gelb and Clark. Identity is a basic means to access many of the rights set out in International Law.[118]

Additionally, as Cartaxo and Simoes argue, the lack of digital identity implies social exclusion as well as the impossibility to participate in citizenship and to take part in social mobilizations. It also prevents sharing global economic development and accessing modern information.[119] Therefore, there is a wide consensus on the role of digital identity as a provider of rights.

Digital identity: a threat to rights?

Digital identity systems and procedures might affect or even damage human rights. In its Guidelines on National Digital Identity, the Consultative Committee of the Convention of the Council of Europe had already warned about the adverse consequences of digital identification for human rights. Besides privacy risks, these implications can 'range from discrimination and exclusion to marginalization, to unwarranted profiling and surveillance, to a person's loss of control over their identity or even the misuse or theft of one's identity'. Actually, national digital identity schemes 'may not appropriately consider, provide for or safeguard against risks to the fundamental rights and freedoms of individuals'.[120] Beduschi and Walshe have analysed the effects of digital identity technologies in particularly complicated cases such as the Rohingya minority in Bangladesh or the Uyghurs in China.[121] A general and basic aim must be to avoid digital identity being commodified and to prevent that 'being human' means becoming machine-readable and profiled bodies.[122]

More specifically, a main problem arises from the use of digital identity as a means of control and surveillance. It is a complex debate. Martin argues that it clearly enables super-surveillance,[123] while Blackman holds the theory that the solution against omni-vigilance would

[114] Manby (n 92) 2–3.

[115] Szreter argues that digital identity is of central significance for human rights and development by stating that 'without the legally sanctioned, secure, and practically available capacity to prove one's identity, the political rhetoric of human rights, and the academic discourse of entitlements, functioning, and capabilities remains, at best, a set of ideals and aspirations for the world's anonymous poor' (Szreter (n 105) 68).

[116] Following Aresty, 'recognition as a person with rights and duties is a fundamental aspect of identity, because it enables a person to enjoy associated elements that determine daily life and individuality'. Among these rights, he mentions 'the right to life and to personal integrity as enshrined in Article 6 paragraph 1 ICCPR, as well as prevention from arbitrary arrest as enshrined in Article 9 paragraph 1 ICCPR; The right to privacy and family life that includes the protection of honor and confidential correspondence as enshrined in Article 17 ICCPR; The freedom of thought, conscience and religion as enshrined in Article 18 paragraph 1 of the ICCPR: this fundamental right attaches to the non-physical identity; The freedom of expression as enshrined in Article 19 paragraph 1 and 2 ICCPR. Furthermore, minority rights as individual rights to practice culture and religion are granted to persons who belong to a certain group identity as enshrined in Article 27 ICCPR. Finally, in democratic countries legal identity also extends to political identity and includes the right to vote and to be elected' (Aresty (n 31) 141–142).

[117] Clare Sullivan, 'Digital Citizenship and the Right to Identity in Australia' (2013) 41 (3) Federal Law Review 560–561.

[118] Among those rights, they include 'a name, an identity with family ties, nationality, recognition before the law, participation in electing government, take part in government, own property, and to equal access to public services as well as social security' (Alan Gelb and Julia Clark, *Identification for Development: The Biometrics Revolution* (2013) 8, avalaible at https://www.cgdev.org/publication/identification-development-biometrics-revolution-working-paper-315).

[119] Geovana M. Cartaxo de Arruda Freire and Tainah Simoes Sales, 'Os direitos à identidade digital e à acesso a internet como instrumentos de concretiçao dos objetivos de desenvolvimento do milênio e da democracia' (2015) 29 (3) Justiça do Direito 564.

[120] Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data of the Council of Europe (n 25) 6.

[121] Beduschi (n 78) 1; Walshe (n 2) 19–21.

[122] Walshe (n 2) 22. According to the Consultative Committee of the 108 Convention of the Council of Europe, 'make people "machine readable" carries the risk of reducing people to a mere object removed from considerations of human dignity and other adverse consequences for their human rights and fundamental freedoms' (Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data of the Council of Europe (n 25) 6).

[123] According to Martin, 'both government and commercial actors had seized the opportunity presented by a perceived security crisis to justify a range of identification and surveillance interventions, including new identity technologies for citizens and foreigners/visitors alike; the use of biometrics across different sites, especially at borders; and increased sharing of personal data between international actors. Our societies are still experiencing the broad effects of these securitized identification interventions' (Aaron Martin, 'Aadhaar in a Box? Legitimizing Digital Identity in Times of Crisis' (2021) 19 (1) Surveillance & Society 104).

be 'the right to your digital identity' established as a new tort.[124] According to Weitzberg *et al.*, these are not the two sides of a binary debate, but 'mutually compatible developments that are increasingly collapsed (…) Identity technologies have opened avenues for formal claims-making just as they have enabled extractive and intrusive forms of monitoring'.[125] Biometric identification appears to be the most complicated issue in this regard.[126] Weitzberg *et al.* have precisely examined the use of this methodology in the case of refugees warning about the dangers of surveillance humanitarianism.[127]

There are different systems, procedures and methods of digital identification. Some may indeed represent a threat or even compromise fundamental rights. However, there are others which provide higher levels of protection of these rights, such as the credential models and, in particular, the self-sovereign identity system, for instance. There is general consensus about preventing threats and risks to human rights. However, many countries, ranging from undemocratic to democratic, are turning to biometric techniques for digital identification, sometimes for economic reasons including the possibility of monetizing identity.

Digital identity, economy, and development

There is agreement on the key role played by digital identity in the fields of economy and development, which surpasses the capabilities of its physical antecedent. However, there are also areas of concern and negative aspects.

Digital identity and economy

Digital identity is critical for the economy. Takemiya and Vanieiev argue that it is the cornerstone of digital economy.[128] In a similar way, Al-Khouri,[129] Smedinghoff,[130] Pato,[131]Lips,[132] Sule *et al.*,[133] Tammpuu and Masso,[134] and the Boston Consulting Group[135] have highlighted the economic value of digital identity. By 2020, the digital identity market was expected to be worth between $16 billion and $22 billion, and it continues to grow.[136] However, digital identity business is not trouble free.

According to Knight and Saxby, there is a growing monetization of digital identities in a transactional sense, to the extent that identity is touted as the new money.[137] Zumbansen states that

[124] Josh Blackman, 'Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity: Tort for Recording and Disseminating an Individual's Image over the Internet' (2009) 49 (2) Santa Clara Law Review 314.

[125] Weitzberg *et al.* (n 1) 2.

[126] Niloufer Selvadurai, 'Not just a face in the crowd: addressing the intrusive potential of the online application of face recognition technologies' (2015) 23 (3) International Journal of Law and Information Technology 187–218; Gary Kok Yew Chan, 'Towards a calibrated trust-based approach to the use of facial recognition technology' (2021) 29 (4) International Journal of Law and Information Technology 305–331; Gelb and Clark (n 118) 8.

[127] Weitzberg *et al.* (n 1) 3.

[128] Takemiya and Vanieiev (n 13) 582–587.

[129] Ali M. Al-Khouri, 'Digital Identity: Transforming GCC Economies' (2014) 16 (2) Innovation: Management, policy & practice 184.

[130] Smedinghoff (n 90) 555.

[131] According to Pato, 'identity management systems are fundamental to underpinning accountability in business relationships; providing customization to user experience; protecting privacy; and adhering to regulatory controls (…). Identity Management is the set of processes, tools and social contracts surrounding the creation, maintenance and termination of a digital identity for people or, more generally, for systems and services to enable secure access to an expanding set of systems and applications' (Pato (n 52) 1).

[132] Lips (n 59) 1.

[133] Following the authors, using digital identity, the states 'can build a comprehensive profile on the political, educational and economic behaviors of their people, thereby aiding the nation in planning and addressing the needs of its citizens' (Sule, *et al.* (n 74) 2).

[134] Pila Tammpuu and Anu Masso, 'Transnational Digital Identity as an Instrument for Global Digital Citizenship: The Case of Estonia's E-Residency' (2019) 21 Information Systems Frontiers 622–623.

[135] Boston Consulting Group (n 75).

[136] Gstrein and Kochenov (n 19) 2.

[137] Knight and Saxby (n 17) 620.

'the panopticon is everywhere and every single aspect of their identity and movements is being commodified by someone'.[138] Walshe believes that the emergence of ever more intrusive digital identity technologies is leading to the commodification of legal identity.[139] Teller concludes that 'the patrimonialisation of the self is made possible'.[140] Such a situation raises fundamental dilemmas. Digital identity goes well beyond the purely economic issue with a definite impact, in particular, in the field of development.

Digital identity and development

Digital identity has different and controversial functions in the area of development. As is well known, previous systems of legal identification have not been able to eliminate or reduce the so-called identity gap. In many countries, a lack of identity is equivalent to a lack of rights and even directly to non-existence. According to Gstrein and Kochenov, if technology is taking the side of the current status quo or it is not able to reverse this situation, 'it will most probably emerge as yet another, immensely effective tool of oppression and injustice'.[141]

The interplay between digital identity and development has been highlighted through various arguments by Gelb and Clark,[142] Masiero and Bailur,[143] or Addo and Senyo,[144] among others. Although not enough research has been done yet to explain the real scope of this link, according to statistics, it seems that more than15 per cent of the world's population are unable to reap the benefits of development because they have no means of proving their legal identity. It is a systemic identity gap that poses a challenge to human development and not just to economic growth. Such an identity gap is increasingly recognized not only as a symptom of underdevelopment but as a contributing factor to it.[145] According to the available data,[146] more and more countries in Africa, Latin America, and Southeast Asia are already implementing digital identity systems to tackle this problem.[147]

Digital identity and development have been widely analysed in the academic sphere providing complementary arguments and approaches. Firstly, digital identity offers the possibility of holding fair and democratic elections and fostering national unity that is a key factor for development.[148] Secondly, it can provide adequate public administration[149] and bring important

[138] Peer C. Zumbansen, *Law's New Cartographies Spatialization, Digital Borders and Spaces of Vulnerability*, (2022) 25.

[139] Walshe (n 2) 6.

[140] Marina Teller, 'Legal Aspects Related to Digital Twin' (2021) 379 Philosophical Transactions 20210023 2, available at https://doi.org/10.1098/rsta.2021.0023.

[141] According to the authors, 'while particularly people from developed countries take their privileged status for granted, citizenship remains one of the most crucial global instruments for upholding and reinforcing inequalities through installing (often impenetrable) barriers in a world where inequalities are rooted more in space than in class. Arguably, manifested in traditional identity management systems such as passports, glass ceilings are distributed among the human population, in many ways emerging as the core element of the contemporary world order… one might propose that such behavior is opposed to the enlightenment ideal of equal human worth, the idea of deserving and rationality, as well as the concept of human dignity, which is at the core of modern human rights law. The current citizenship system can be considered as a rigid cast system. If technology is uncritically taking the side of the current status quo, instead of offering new rationales to question it, it will most probably emerge as yet another, immensely effective tool of oppression and injustice' (Gstrein and Kochenov (n 19) 2).

[142] Gelb and Clark consider the 'identity gap' as human rights and development issues. In addition to the fact that the development goals of a country can equally be seen as development aspirations for its citizens, identity is central to provide the ability of countries and governments to deliver services to their citizens (Gelb and Clark (n 118) 8).

[143] They argue that identity provides the basis for people to have rights, receive public services, or benefit from much-needed forms of social assistance (Masiero and Bailur (n 95) 1).

[144] Atta Addo and P.K. Senyo, 'Advancing E-governance for Development: Digital Identification and its Link to Socioeconomic Inclusion' (2021) 38 Government Information Quarterly 101568 1–2.

[145] Gelb and Clark (n 118) 52.

[146] ITU-T Focus Group Digital Financial Services, *Review of National Identity Programs* (2015), available at https://epar.evans.uw.edu/sites/default/files/EPAR_UW_Request_306_National_Identity_Programs_11.11.15_0.pdf; World Economic Forum (2016). *A Blueprint for Digital Identity. The Role of Financial Institutions in Building Digital Identity* (2016), available at https://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

[147] Addo and Senyo (n 144) 2.

[148] ITU-T Focus Group Digital Financial Services, *Review of National Identity Programs* (2015), available at https://epar.evans.uw.edu/sites/default/files/EPAR_UW_Request_306_National_Identity_Programs_11.11.15_0.pdf

[149] Gstrein and Kochenov (n 19) 2–3.

organizational, economic, political, as well as social changes on a large scale in a relatively short period of time.[150] Thirdly, it is an optimun way to put technology at the service of socio-economic development[151] and governance.[152] This is why digital identity is now firmly anchored in the development agenda.[153]

Moreover, in the context of development, digital identity appears to have additional functions to those attributed to it in developed countries. Commonly, digital identity is linked to the aim of digitalizing and improving access to goods and services. By contrast, in developing low-income countries, the primary aim of digital identity is still basic identification, especially in cases where earlier physical identity systems were inefficient or absent.[154] Although there are several levels of identity coverage,[155] digital identity seems to be the way to overlap the identity gap. Indeed, it fulfils different functions in different contexts.[156] Sometimes it can even serve conflicting functions.

Digital identity: an inclusion or exclusion driver?

Digital identity can be a tool for inclusion or exclusion. Addo and Senyo and Weitzberg *et al.* have defended its value for inclusion since it allows more efficient administration of public services, more transparent decisions and governance, and more accurate measurement of development progress.[157] However, digital identification can also become a means for exclusion.

As Gelb and Clark explain, for many people, identification raises concerns about 'government encroachment on citizen's rights and is associated with victimization, oppression, and exclusion. Biometric-enabled identification elicits similarly opposing viewpoints; some see it as a means to improve services, others associate it with an Orwellian dystopia.'[158] According to Masiero and Bailur, identity enables human freedom in one sense although it can also restrict it 'depending on who is doing the identifying'.[159]

Gelb and Metz admit that there is no single formula for identification systems, since exclusion, misuse, corruption, or waste of investment are real risks, especially, but not only, in developing countries.[160] Gstrein and Kochenov argue that the true problem derives from the existing

[150] Addo and Senyo (n 144) 12.

[151] Masiero and Bailur define digital identity as an emerging way to put technology at the service of socio-economic development. Citing the World Bank as their source, the authors recognize three main aims of digital identity concerning development: (i) Inclusion and access to essential services; (ii) More effective, efficient, and transparent administration of public services; and (iii) More accurate measurement of progress according to key development indicators (Masiero and Bailur (n 95) 2).

[152] Addo and Senyo offer two arguments for addressing the digital identity gap by connecting development and governance. First, digital identity provides an efficient and cost-effective tool to make visible people who would otherwise be unknown or invisible and to enable the state to better fulfil its obligations towards them. Secondly, digital identity could overcome many development obstacles related to the lack of legal identity, the absence of national standards of identification and authentication or the unavailability of a centralized registry of individuals within the countries (Addo and Senyo (n 144) 9–10).

[153] Alan Gelb and Anna D. Metz, *Identification Revolution: Can Digital ID Be Harnessed for Development?* (Center for Global Development, GD Brief October 2017) 1, available at https://www.cgdev.org/sites/default/files/identification-revolution-can-digital-id-be-harnessed-development-brief.pdf

[154] Tammpuu and Masso (n 134) 623.

[155] According to Gelb and Metz, 'early adopters with widely used, high-coverage ID systems include Peru, Pakistan, Thailand, and Rwanda. India's Aadhaar program has enrolled close to 1.2 billion. At the other end of the spectrum, poor and conflict-affected countries like Somalia, Liberia, South Sudan, and the Democratic Republic of Congo start out with few identity management assets. Many of their residents have never been formally registered; as a result, there is no comprehensive population registry to support social programs or verify residents' identities. Countries like Nigeria, Ghana, and the Philippines have multiple disconnected systems for voting, healthcare, tax administration, and other purposes. Each service provider and public entity maintains its own registration process and database at significant cost. Often, systems fail to follow common standards and may not be technically interoperable. A fourth group, including Kenya and Zambia, has reasonably robust systems whose capabilities could be boosted by new technologies. Transitioning from paper-based records to more easily manageable digital systems, and improving the identity verification infrastructure, could, for example, boost the efficiency and accountability of service delivery' (Gelb and Metz (n 153) 3).

[156] Rodrigues recognizes that it is a fragmented and changing category that, despite being a technical construct, is influenced by local conditionality (Rodrigues (n 12) 6–7).

[157] Addo and Senyo (n 144) 2.

[158] Gelb and Clark (n 118) 12.

[159] Masiero and Bailur (n 95) 2.

[160] Gelb and Metz (n 153) 4.

real-world inequalities. Since citizenships can be used to exclude, to be identifiable is not necessarily 'a good thing'.[161] As can be seen, digital identity raises important dilemmas of a functional nature in basic areas such as human rights, economy, or development.

CONCLUSIONS

Digital identity has its roots in the original identity designed in the physical world, not always, not necessarily, and not exclusively circumscribed to the legal framework. It is not the first and will not be the last complex and multifaceted category which, for its regulation and beyond regulation, requires the assumption that it is a polyhedric reality. It demands an interdisciplinary approach because it has a wide-ranging scope and a variety of background consequences which can be philosophical, psychological, sociological, anthropological, or ideological, as well as economic, political, and social.

In the physical world, identity has a legal foundation and a legal status in many juridical systems in which it constitutes the normative basis certifying the existence of a subject and the legal personality that enables the exercise of rights and the fulfilment of duties. There are countries, such as the UK, that do not use this institution. Some African countries have been trying for years to overcome the identity gap that is an additional factor feeding underdevelopment. In spite of this situation, as demonstrated by the fact that there are people in these countries without a legal identity, in the physical world legal existence does not always depend on legal identification. Instead, accessing and participating in the digital world requires the use of a digital identity offered by states, and also by private providers. In the pre-digital world, this situation was normal, but the value and meaning of public identity were not equivalent to that of private identifications used to obtain access to a library, a club, or any particular association. In the digital context, the accreditation of identity by a country has a scope of application potentially limited to its territory, while the identification offered by private agents has a transnational scope. In the physical world, it is a medium of identification, while in the digital one, it fulfils three basic functionalities—identification, authentication, and authorization—and is the actual entry point to that ecosystem. In the physical domain, there were homogeneous, standardized, or similar identification procedures. In contrast, the models of digital identity management range from biometrics to computational identity as well as the very diverse models of centralized, federated, decentralized, or self-sovereign credentials. With this background, the present article has examined digital identity through the three main dilemmas it poses according to the normative, the international practice, and the academic doctrine: contextual, conceptual, and functional.

About the contextual dilemma

The context of digital identity is different from the physical world for three structural and several conjunctural reasons. Structural changes are the following: (i) It is a digital scenario; (ii) It requires the creation of identities in order to access and participate in it; and (iii) It is a space integrated in others. Although cognitively useful, the artificial division between a physical and a virtual world is neither real nor useful, because both interact and operate connected within the global ecosystem. Digital identity, for instance, allows access to both physical and digital goods and services.

Conjunctural changes include the need to accommodate both technical and legal requirements to build digital identities; the demand to distinguish and coordinate identity procedures for humans, devices, and processes; the main value of secure and reliable methodologies; the monetization of identity; the privatization of digital identity services; and the extreme

[161] Gstrein and Kochenov (n 19) 6.

fragmentation of the digital identity landscape. In this context, digital identity is a different and singular category. It requires an appropriate legal framework, even one particularly qualified and protective since it is the path to access the digital world and to exercise basic rights through it. In this context and in the face of these changes, digital identity cannot be analysed by simple analogy with its legal precedent, but requires a different approach, starting with its concept.

About the conceptual dilemma

Digital identity has been described as social, subjective, valued, referential, composite, consequential, dynamic, contextual, ambiguous, unitary or multiple, equal or different, fixed or flexible, local or universal, authentic or fictitious, possessed or owned, assigned or assumed, fragmented or cohesive, public or private, anonymous or pseudo-anonymous, temporary or permanent, and visible or invisible. In addition, it is a universal concept able to serve different functions in different contexts and a fragmented, layered, composed, multifaceted, changing, and dynamic category. These features not only diverge from those of the traditional idea of identity but may also explain the difficulty of reaching an agreement on its concept.

Proposals for its definition include those who consider it impossible—it is not an option in scientific terms-, those who consider it a mixture of individual determination and relational aspects—it is not a choice that can be translated into legal terms-, and those who support definitions based on the idea of representation, information or data or both representation and information or data. The concept of digital identity cannot be defined in abstract or technical terms without considering the consequences from a legal point of view. Although it may be difficult—and definitions by definition may be restrictive or limiting-, the concept of digital identity must be defined precisely because this is the determinant factor for establishing its legal framework. Conceptualizing it as representation, information or data, or both, is not the same, because this substantially changes the legal framework. The idea of representation is graphic, metaphorical, although insufficient and inadequate since digital identity always implies information and data. Information and data—which are personal from the moment they enable a person to be identified—constitute a basic component of the concept of digital identity. To the extent that it involves personal data and privacy, such a concept needs a specific and qualified legal framework in order to protect these rights and juridical assets. Going deeper into the analysis, the concept of digital identity appears to be dual. It is both a substantive and an instrumental concept because it fulfils three basic technical functions: identification, authentication, and authorization. In addition to them, digital identity can develop different functions in different areas.

About the functional dilemma

Human rights, economics, and development are three essential areas of action, and specific branches of law, within the framework of International Law that are being used in order to demostrate the dilemma at hand. In each of them, the potential of digital identity to achieve different or even contradictory functions has been considered. It can serve for inclusion or exclusion, but it is a valuable tool for development. It is a factor behind economic growth and it is also an economic value which poses the risk of commodifying or patrimonialising identity. It can be, for that and other reasons, a threat or a danger to certain basic rights, including human dignity. It is also, however, an instrumental right, a provider of rights, insofar as it enables access to and exercise of other rights, even human rights such as freedom of expresion or information. Recognizing digital identity as an autonomous right could serve to prevent its use for exclusion in the field of development, its commodification in the economic sphere, or its threat to other basic rights.

After considering these three dilemmas and prior to the discussion of whether it is an autonomous right or not, the concept of digital identity must be the priority. In order to determine its legal framework, it is necessary to know what it is. The definition has to include the substantive component—information and data—the functional component—since it is used to fulfil the functions of identification, authentication, and authorization—the theological component—in order to access and participle in the digital world—and the ontological component—because digital identity is itself an attribute-. It is a property or an entitlement that enables us to do something: to fulfil those functions and to achieve that goal. Therefore, digital identity could be defined as an attribute composed of information and data that enables identification, authentication, and authorization for access and participation in the digital world.

The legal framework of digital identity has to be designed taking into account the following components: (i) Normative concerning personal data protection and privacy because digital identity provides information and data and operates through electronic means. A different legal regime could be established if it is a natural or legal person or an object, whose data may or may not be personal depending on whether or not they can be associated with a person; (ii) Normative regarding identification, authentication, authorization and certification processes and tools, certificates and electronic signatures, including the technical standards for defining digital identity management models; (iii) Norms concerning the security of networks and information and communications systems and services to ensure reliable and secure connections, transmissions and transactions; and (iv) Regulations on interoperability and/or mutual recognition of digital identification systems since there are different models and digital identity has to be used at a transnational level. Fundamental rights and freedoms must obviously be the basic legal framework for the development of digital identity models.

Finally, three general problems of major relevance and complexity need to be addressed. Firstly, the issue of the privatization of digital identity systems must be analysed, not only as a problem linked to this area, but also as a phenomenon embedded in the processes of globalization and technification. Campione has warned about the displacement of social power implied by such management of digital identities by private actors who occupy a prominent position in the markets.[162] Benvenisti highlights the same problem concerning the privatization and monopolization of the communication space.[163] Secondly, commodification and monetization of digital identity by external providers, public or private, or by the identity holders themselves, must be carefully analysed. There is even a need for a fundamental debate pointing to the concept of dignity when, as Teller observes, 'the patrimonialization of the self is made possible'.[164] Thirdly, it is important to rethink and reformulate normative processes in order to avoid this paradoxical phenomenon whereby technical norms precede and seem to determine the scope, content and meaning of legal norms. The technical aspects of digital identity models are an obvious and natural driver for their legal regulation. However, it has to be the legislator and the norm who determine the premises on which the standard has to be based instead of having technical standards—defined by technical as well as private bodies—establishing the criteria on which the legal norm must operate. Privacy by design, for instance, is a requirement that would actually fulfil its functionality if the idea of privacy were legally interpreted in the context of digital identification by law, rather than placing that responsibility on those who have to implement it technically but do not necessarily have the legal expertise and certainly do not have the proper legitimacy to ascertain the meaning of that right in this context. Public–private cooperation is essential, as is the contribution of standardization bodies, but with a clarification

[162] Roger Campione, *La plausibilidad del derecho en la era de la inteligencia artificial. Filosofía carbónica y filosofía silícica del derecho* (Dyckinson 2020) 20.

[163] Benvenisti (n 27) 71.

[164] Teller (n 140) 2.

of the processes and their respective roles. Technological solutionism can never be the answer to the complex problems, not just legal, posed by digital identity.

FUNDING

This article has been published under the research project PID2020-114495RB-I00 funded by MCIN/AEI/10.13039/501100011033. Funding for open access charge: Universidad de Granada/CBUA.