European Review of Digital Administration & Law - Erdal
2021, Volume 2, Issue 2, pp. 75-87
ISSN 2724-5969 - ISBN 979-12-5994-752-9 - DOI 9791259947529 09

*Allocating Control in Decentralised Identity Management**

Alexandra Giannopoulou
(Postdoctoral Researcher, Institute for Information Law, University of Amsterdam)

ABSTRACT Creating legal identity in the digital space involves the challenging task of addressing the data-related responsibilities and obligations for data governance and data protection (by design and by default) to name a few. Substantially, it also requires the datafication of legal identity which means transposing all its properties and foundational traits inits corresponding data expressions and relations. As (digital) legal identity evolves from the fringes of purely technology-related challenges towards the legal and socio-technical, state institutions –sovereignly responsible for delivering digital legal identities to citizens– are acknowledging the polyvalent, non-monolithic, and relational characters of identitiesand they explore appropriate architectures. This paper sets out to explore the institutional turn towards decentralized digital identities. The claims surrounding these digital identities raise high hopes for the cross border digital identity provisioning being data protection and privacy compliant, technologically secure, and user-centric. This paper attempts to explore how the relevant accountable actors –as recognized through the data protection normative framework– are formed around the technological identity infrastructure.We highlight and examine the conflict between the European proposals on the provision of digital identity infrastructures through decentralized architectures and the concepts of data controllership in the GDPR.

1. *Introduction*

In the State of the Union speech on 16 September 2020, the President of the European Commission put digital identity provisioning at the heart of the Commission's ambitions: "We want a set of rules that puts people at the centre. (...) This includes control over our personal data, which we still have far too rarely today. Every time an app or website asks us to create a new digital identity or to easily log on via a big platform, we have no idea what happens to our data in reality. That is why the Commission will soon propose a secure European e-identity. One that we trust and that any citizen can use anywhere in Europe to do anything from paying your taxes to renting a bicycle. A technology where we can control ourselves what data and how data is used"[1]. This ambition was later affirmed and solidified by the European Council's support which, in its Conclusions of 1-2 October 2020, highlighted the need for the European Commission to put together a European digital identity framework proposal. Namely, the European Council called for "The development of an EU-wide framework for secure public electronic identification (eID), including interoperable digital signatures, to provide people with control over their online identity and data as well as to enable access to public, private and cross-border digital services". The Council invites the Commission to "come forward with a proposal for a European digital identity framework initiative by mid-2021"[2].

In its most recent communication, the European Commission announced the following strategic goal: "Government as a Platform is the new way of building digital public services. The ambition is that by 2030 all online provisions of key public services become available for European citizens and businesses, that all European citizens have access to their medical records (e-records) and that 80% of citizens will use a digital ID solution"[3]. In this phrasing, it clarifies that the path towards achieving a European digital ID will be facilitated by the European Health Data Space project. The proposal for a Regulation on the European Health Data Space[4], this regulatory instrument is planning

* Article submitted to double-blind peer review.

[1] U. Vor der Leyen, *State of the Union Address by President at the European Parliament Plenary*, 16 September 2020, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655 (last access: 4 May 2022).

[2] European Commission, *Report from the Commission to the European Parliament and the Council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)*, Brussels, 3 June 2021, COM(2021) 290 final, §1.2.

[3] European Commission, *Proposal for a decision of the European Parliament and of the Council establishing the 2030 Policy Programme "Path to the Digital Decade"*, Brussels, 15 September 2021 COM(2021) 574 final 2021/0293 (COD). See also the 2020 *Berlin Declaration on Digital Society and Value-Based Digital Government*.

[4] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the*

to "build upon the new proposal on the European Digital Identity with the improvements in the domain of electronic identification, including the Digital Identity Wallet". The European regulator attempts to address electronic identification and digital identity as a technological infrastructure which can be built with individual control as a fundamental principle and which can facilitate cross-border identity verification in a secure, interoperable manner. This narrative is critical for our paper, which sets out to explore the institutional turn towards decentralized systems for digital identities.

The claims surrounding digital identities raise high hopes for the cross border digital identity provisioning being data protection and privacy compliant, technologically secure, and user-centric. This paper attempts to explore how relevant accountable actors –as recognized through the data protection normative framework– are identified around this decentralized technological identity infrastructure. The allocation of control within a decentralized digital identity system should reflect the responsibility that the government and European institutions have (or should have) in the creation of digital identity and its corresponding technological infrastructures. We critically approach the conflict emerging between European proposals on the provision of digital identity infrastructures through decentralized architectures and the GDPR concept of data controllership. As explained in our analysis, the deployment of decentralized technological infrastructures for digital identity systems presents certain advantages compared to others but, when constructed by European institutions and/or Member States, there is an equal need to ensure that accountability be properly maintained by the relevant corresponding institutions in these systems.

Identification management systems allow the establishment of trust relationships[5] especially between sovereign states and their citizens. In general, identity is considered a fundamental element in promoting social equality, freedom, democracy and economic independence. For this reason, the organization of identification systems and the definition of certain universal rules of operation both constitute essential preconditions to the digitalization processes of citizens' interactions with the state and with the private sector. The importance of trust in these interactions cannot be overstated: on the one hand, the issuance and recognition of the validity of various aspects of our identity (national identity cards, passports, driver's license, etc.) lies within the sovereign powers of a state. On the other, in the private sector, various forms of digital identification offer access to products, services, or even specialized privileges (for example: email accounts, social media, bonus cards, and membership cards, etc.). This means that digital identity appears in different forms as a necessary technological artefact underlying many functions of our everyday lives.

The management of digital identity –similar to that of non-digital identity– is subject to national regulations, as an expression of the sovereignty of the digital state[6]. However, there is a growing need for the delivery of cross-border digital services and digital interactions between Member States' citizens, businesses, and public authorities. For this reason, the creation of a cross-European digital identity infrastructure became a priority in the European Digital Strategy. In a recent statement, the European Commission stated that "a universally accepted public electronic identity (eID) is essential for consumers to have access to their data and to use the products and services they want without having to use irrelevant platforms. to do so and unnecessarily share personal data with them. Europeans can also benefit from the use of data to improve public and private decision-making"[7]. Similarly, the European Strategy for the Digital Financial Sector states that "by 2024, the EU should implement a sound legal framework that allows the use of interoperable digital identity solutions", which

European Health Data Space, COM/2022/197 final.

[5] B. Manby, *Legal Identity for All' and Statelessness: Opportunity and Threat at the Junction of Public and Private International Law*, in *Statelessness and Citizenship Review*, vol 2, issue 2, 2020, 248-271, and B. Manby, *The Sustainable Development Goals and "Legal Identity for All": "First, Do No Harm"*, in *World Development*, 2021, 139, https://doi.org/10.1016/j.world dev.2020.105343.

[6] T. Madiega, *Digital sovereignty for Europe*, in *European Parliamentary Research Service Ideas Papers*, vol.10, issue 2, 2021.

[7] European Commission, *Commission proposes a trusted and secure Digital Identity for all Europeans*, Press release, 3 June 2021 https://ec.europa.eu/commission/ presscorner/detail/en/ip_21_2663.

will lead to consolidation of universal technological rules, interoperability and wider security in the identification and authentication of users by financial institutions (and beyond).

Identification and identity construction processes are all the more becoming digitalized. Identity has become a commercial matter and not just one performed by public institutions. As a result, identity has increasingly become a technological artifact[8], a digital solution aspiring to formalize the individualization of access to computer networks and to digitally recreate the relationships that (in)form identity. Khatchatourov describes the double essence of the concept: "Digital identity can therefore have two complementary meanings, which precisely constitute the crux of the problematic of this domain: identification of the user and their actions in the digital environment and the effects of digital technology on the construction of identity understood as a relationship to oneself, to others and the public space".[9]

On a European level, this ongoing process of digitalizing identity is supported by a network of regulatory reforms, and is facilitated by targeted technological change. As evidenced and highlighted by the European Commission, these processes are intensifying at the aftermath of the pandemic: "In just one year, the COVID-19 pandemic has radically changed the role and relevance of digitalization in our societies and economies, and accelerated its pace. In a response to the increased digitalization of services, the demand by users and business for means to identify and authenticate online, as well as to digitally exchange information related to identity, attributes or qualifications, in a secure way and with a high level of data protection, has increased radically"[10].

Digital identity has been identified as an essential component for securing a single digital market, and an institutional European goal that seeks appropriate and proportionately necessary technological integration. As part of its Digital Agenda program, the European Commission announced on 3 June 2021 the goal of creating a "European digital identity" which "will be available to EU citizens, residents and businesses wishing to prove their identity or to confirm certain personal information. It can be used for both online and offline public and private services across the EU". This digital identity project envisages the integration of digital identity wallets, which would function as a local (on citizens' phone devices) digital storage of identity credentials from public and private trusted (identity) sources. This initiative aligns with the broader network of products, services, and infrastructure that the European Union is undertaking in order to facilitate cross-border interoperability of national digital identities. This article explores how responsibility can be allocated according to the GDPR on decentralized digital identities.

2. *Towards a decentralized digital identity framework*

The lack of a persistent and horizontal digital identification layer online can be (and has been) perceived as a technological feature favoring anonymity and pseudonymity. However, the need to create an identification technical layer for every online service added to the complexity in network-mediated services and relations[11]. The lack of technical standardization in identity provision has enabled the rapid growth of digital identity markets, which has grown into a multi-billion-dollar industry. There is no shortage of technical specifications, tools, standards, and certification mechanisms online, all attempting to provide the most suitable technological solution to digital identification. Admitting the limitations of the current web 2.0 digital identification implementations, the vision for the web 3.0 describes a digital identity management system that prioritizes decentralization, interoperability, and user control. This vision is also adopted by the

[8] Since the early '90s, Donna Haraway spelled out a 'cyborg' identity, to highlight that it would be increasingly difficult to discern where the individual ends and where the machine begins. D. Haraway, *The Cyborg Manifesto. In: Simians, cyborgs, and women: the reinvention of nature*, London, Routledge. 1991, 149-182.

[9] A. Khatchatourov, *Digital identities in tension. Between autonomy and control*, Hoboken, NJ, Wiley, 2019, 24.

[10] European Commission, *Recommendation on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework*, Brussels, 3 June 2021, C (2021) 3968 final.

[11] I. Kerr, C. Lucock, and V. Steeves, *Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society*, Oxford, Oxford University Press, 2009.

European Commission which states: The "provision of digital identity is undergoing fundamental changes. Entities such as banks, providers of electronic communications services or utility companies, some of which are required by law to collect identity attributes, are leveraging their procedures to act as verified identity providers. Internet intermediaries, including major social media platforms and internet browsers, act as de facto digital identity gatekeepers and offer BYOI (bring your own identity) solutions that allow their users to authenticate on third-party websites and services by using their user profiles. This convenience comes at the cost of loss of control over disclosed personal data while these eID means are disconnected from a verified physical identity, which makes fraud and cybersecurity threats more difficult to mitigate. A large majority of EU citizens would like to have access to a secure digital identity that they could use to access online services. Finally, although there are many different views on the future of digital identity, the key role of the national governments in the development of any far-reaching digital ID ecosystem needs to be duly considered". The European Commission highlights the role national governments have to play in digital identity provisioning, and it positions all of them as key players in the creation of the European digital identity ecosystem, based on a decentralized identity infrastructure.

As evidenced above, digital identity reforms tend to focus their efforts on developing open technical standards and ensuring interoperability on the one hand, and on escaping the control of dominant identity providers on the other. The emphasis on decentralization as a technological design principle, stems from risks and limitations that prior established digital identity management systems operating both in the private and public sector have identified.

By identity management, we refer to the centralized management of multiple identities, perceived as authentication and access control systems, online. This means that a considerable number of an individual's (social) identification online is/can be mediated through a single Facebook or Google account. Similarly, in the public sector and provision of e-government services, digital identity management is mediated through a single application. In the case of the Netherlands, for instance, this means the DigiD[12].

These different identities, mediated by different identity providers but often founded on similar technological architectures, can be used to authenticate users/citizens so that they can access different services with various service providers. Identity management "allows users to manage their online identities but also allows service providers to determine the conditions under which users get access to their services"[13]. However, the increased centralization of identity provision through existing identity systems was identified as both a privacy and a security risk[14].

Decentralized identity technological infrastructures are emerging as ways out of these risks. However, as we have already noted elsewhere, "decentralization in the technology discourse is rarely a descriptive category with its own particular costs and benefits, but rather a normative ideal. Centralization means the rule of the few over the many, the potential for censorship, for coercion. Decentralization is seen as the architectural guarantee of censorship resistance, and a safeguard against the coercive influence of any centralized, top-down force. The external forces of control –institutions, intermediaries, rules, laws, and norms– prevent the ideal, purely technological modes of private ordering, based on the horizontal self-organization of equal peers"[15].

Lately, the mythical objective of decentralization has been intrinsically linked with blockchain-based systems. More importantly, digitization of legal identities is becoming one of the main domains of development for blockchain enthusiasts, promising to deliver national and cross-border identity services and infrastructure. Progressively, blockchain-based digital identity solutions solidify their position in the global digital identity market[16]. They also start

[12] https://www.digid.nl (last access: 25 November 2021).

[13] J. H. Hoepman, *Privacy is hard and seven other myths. Achieving privacy through careful design*, Boston, MA, MIT Press, 2021, 132.

[14] *Ibidem*, 127-136.

[15] B. Bodó and A. Giannopoulou, *The logics of technology decentralization: The case of distributed ledger technologies*, in M. Ragnedda and G. Destefanis (eds.) *Blockchain and web 3.0: Social, economic, and technological challenges*, London, Routledge, 2019, available on https://doi.org/10.4324/9780429029530-8.

[16] D. Reed, and A. Preukschat, *Self-Sovereign Identity*, New York, NY, Manning, 2021.

to, in parallel, become associated with government digital identity reforms operating both at a Member State and an EU-level. For instance, on a European Union level, the newly-formed body called European Blockchain Partnership (hereinafter EBP)[17] which is supported by the European Commission, initiated the creation of the European Blockchain Services Infrastructure (hereinafter EBSI)[18]. EBSI is a joint initiative from the European Commission and the EBP to deliver EU-wide, cross-border public services with the use of blockchain technology. EBSI will be composed of a network of distributed nodes spread across European Member States with the participation of the European Commission, leveraging several applications focused on specific use cases[19].The goal of its design is to provide "cross-border process carried out by [national] public authorities, a public service or a service of public interest offered to users (public authorities, companies or individuals) that may be enabled or enhanced by blockchain technology". One of its most heralded use cases is the decentralized (or self-sovereign, to use the established– yet rather misleading term[20]) digital identity framework.

These blockchain-based digital identities are founded on a set of pre-existing technical architectures for identity management, which is on attribute-based credentials. This technological design, later coupled with blockchain-based architectures to form a complete identity management system, is addressing identity as a set of claims that can be reflected on a digital (or physical) credential. These attributes are susceptible to contain any identity-related or identity-relevant information, depending on the context: from driver's license, to passports and university diplomas, attributes are stored in 'digitally signed documents called credentials'[21]. Credentials can be stored at a physical device in a digital wallet or on an external physical storage device. What makes this credential trustworthy and reliable is the encrypted digital signature that secures both the accuracy of the information asserted and its validity as issued by the appropriate and relevant credential issuer. This mechanism exists within (or also without) a blockchain-based system. This mechanism promises to ensure a higher level of security than current identity management systems[22].

For this new technological system to be able to interact with existing institutions embedded within a broader sociotechnical framework, its external recognition to be ensured. This means that the embeddedness, and ultimately the usability of the system in question is dependent on elements such as legal compliance. The drift towards legality "implies that the legal, political, economic systems and institutions develop the necessary tools to adopt the decentralized system. In a similar vein, DLTs also have to build the capacities to be recognizable by existing formal institutions, legal systems. Since legal compliance rests on parties being clearly identifiable, and rights and obligations being well defined, this drift towards legality further creates pathways of recentralization. Control of the blockchain through identifiable actors and processes translates into control of the code, of the network, and/or of the decision-making process"[23].

The reforms announced to deliver cross-border digital identity provisioning promise to develop the relevant EU-wide technological infrastructure in a legally compliant manner. However, to this day, it is still not clear what the legal or technological shape the European digital identity wallet(s) will take.

Decoupling identity provision from identity service providers who tend to abuse their data-driven power is a fair technological aspiration. There are numerous merits in exploring technological design options that could ensure higher security standards for citizen identity data. However, the state sovereign power in issuing legal identities and the government accountability that supports such a power are difficult to apply to decentralization

[17] https://digital-strategy.ec.europa.eu/en/policies/blockchain-partnership (last access: 25 November 2021).

[18] https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure (last access: 25 November 2021).

[19] See https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action (last access: 25 November 2021).

[20] A. Giannopoulou and F. Wang, *Self-sovereign identity*, in *Internet Policy Review*, vol.10, issue 2, 2021.

[21] *Ibid*, 139.

[22] J. Van Dijck and B. Jacobs, *Electronic identity services as sociotechnical and political-economic constructs*, in *New Media & Society*, vol. 22, issue 5, 2020, 896 - 914.

[23] B. Bodó and A. Giannopoulou, *The logics of technology decentralization: The case of distributed ledger technologies*, 114-129.

aspirations. For instance, when operating under “self-sovereign identity” principles[24], these systems aim to distribute technological control over identity data sharing among various ‘nodes’ which maintain the decentralized network. The efforts to eliminate any elements of external control from these identity systems are dominated by technological implementations that see identity management as a set of credential flows and data stored among a complex network of actors[25].

This technical decentralization focus usually influences the governability of the systems in question, complex by nature. Identity management has historically and consistently included many actors with context-dependent accountability, and the articulation of roles in accountability terms often showed its limitations[26]. More importantly, the compliance of digital identity management systems with EU data protection framework is challenging. The allocation of roles such as that of data controllers has often been subject to precise legislative and policy efforts in order to instill legal certainty in the roles and responsibilities of each actor[27].

The significant change that we are observing is the allocation of roles and responsibilities in the redesigned government identity proposals (and their respective cross-border infrastructures), is the shift in the types of actors involved in the identity management networks. In practice, interjecting various private sector technical identity and authentication service providers on a blockchain-based legal identity system creates a complex network of actors that is likely to have the “chain of responsibility and accountability” collapse, “leaving individuals with limited control over how their information is used or any decisions that are made”[28]. For these forms of government digital identities, technologically-mediated and technologically-enabled user control comes at the cost of (legal) clarity and of control-as-in-accountability.

All of the above systems come with assurances of legal compliance which comes with potentially high costs, due to the legal uncertainty in attributing traditional accountability roles in decentralized technological systems developed by both public and private actors. The use of these technological architectures by established institutions with longstanding responsibility affordances can lead to the erosion of trust towards these same institutions[29] every time these technologies show their failures. Technical decentralization through “particular engineering solutions” should not be conflated with “the political, social, or economic aims of decentralization (more autonomy, reduction of power asymmetries, elimination of market monopolies, direct involvement in decision making, solidarity among members of voluntary associations). (…) A decentralized network topology might not produce decentralizing social and political effects and might not even be particularly decentralized in its technical deployment”[30].

Modern digital identity infrastructures emphasize user control, cross-border and cross-sectorial uses, security, privacy, and portability. By focusing on the technical solutions to these aspirations, the public actors sponsoring the integration of these infrastructures remove themselves from the functioning of these systems in their user applications.

[24] This term has been adopted by European institutions in Regulation proposals. See for instance, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity*, 3 June 2021.

[25] Policy and reform of the eIDAS Regulation are an excellent example to showcase this technological focus on identity management. A. Giannopoulou, *Putting data protection by design on the blockchain*, in *European Data Protection Law Review*, 2021, 388-399.

[26] See B. Van Alsenoy, *Data protection law in the EU: roles, responsibilities and liability*, Bruxelles, Intersentia, 2019, 371-374.

[27] However, even in these occasions, the role of institutional actors such as that of the European Commission ends up being an issue of debate. See, for instance, the qualification of the European Commission as an “operator” with specified responsibilities with regard to the IMI system. This dubious characterization was later amended by the EDPS, who qualified the institution as a data controller.

See also B. Van Alsenoy, *Data protection law in the EU: roles, responsibilities and liability*.

[28] E.M. Renieris, *Identity in a “Phygital” World: Why the Shift to Machine-Readable Humans Demands Better Digital ID Governance*, 16 August 2021, available online at https://www.cigionline.org/articles/identity-in-a-phygital-world-why-the-shift-to-machine-readable-humans-demands-better-digital-id-governance.

[29] B. Bodó and H. Janssen, *Here Be Dragons - Maintaining Trust in the Technologized Public Sector*, in *Amsterdam Law School Research Paper*, 2021-23, available at http://dx.doi.org/10.2139/ssrn.3868208.

[30] B. Bodó, J. K. Brekke, J. K. and J. H. Hoepman, *Decentralisation: a multidisciplinary perspective*, in *Internet Policy Review*, vol. 10, issue 2.

The following sections will attempt to showcase the complexities arising in the search for accountable actors (ie principally data controllers) in identity management systems.

3. *Putting (joint) data controllership in context*

In technical terms, digital identity is split across "authentication" (who are you?) and "authorization" (what can you do?). It has been used interchangeably both with technologies of identification and identification management. While the first refers broadly to the practices and technological artifacts used to identify a person, the second describes all technical and organizational processes that ensure that only authorized and authenticated users can get access to the offered services. This conflation of meaning has preoccupied the role, responsibilities, and accountabilities of public institutions and the State, which have systematically been in charge of large-scale data accumulation and which are –by social consensus– established identity providers.

So, digital identity –perceived as the digital representation of different sets of data that can authenticate and assert who is the entity corresponding to that data– is understood as sets of digitally signed certificates. Their validity is highly contingent on the decisive role of a trusted third party and the processes used for identification and for identity management. The dependency to this (at least) tripartite identity flow system, –one that includes the user/citizen/data subject, the identity/certificate issuer, and the receiving authority– is the basis of any digital identity system. What decentralised identity systems aim to achieve, is the centring of identity data flows to the individual and the minimisation of the influence other entities might have on the identity data and their corresponding flows. This aspiration, supported by the corresponding technological design, creates a level of uncertainty on how this system corresponds to an articulation of actors, roles, and responsibilities, especially when examined under the light of data protection regulatory tools.

3.1 *Data controllers in the data protection regulatory framework*

The General Data Protection Regulation[31] describes two types of actors as accountable entities throughout the data processing: data controllers and data processors[32]. This article addresses only the former. The emphasis that the GDPR places on the accountability principle[33], highlighting it as a central tenet, is used to ensure that data controllers "implement appropriate and effective measures" and demonstrate compliance (Recital 4 GDPR). Accountability is introduced as a means to indicate the need for responsible actors to 'self-regulate' and to be able to demonstrate that the related precautionary measures have been takes in line with their obligations from the normative framework.

It is important to highlight the legal distinction between the concepts of responsibility and liability in the specific field of data protection. Put more concretely, the GDPR assigns specific obligations to the responsible entities (responsibility), and when these obligations are not met, then the same legal instrument prescribes measures of liability.[34]

According to article 4(7) GDPR, the data controller is "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law". Appropriate qualification of accountable actors is essential because it will "determine who shall be responsible for compliance with data protection rules, and how data subjects

[31] Hereinafter GDPR

[32] See Chapter 4 (articles 24-43 GDPR).

[33] See B. Van Alsenoy, F. Coudert, L. Jasmontaite and V. Verdoodt, *Cultures of Accountability: A Cross-Cultural Perspective on Current and Future Accountability Mechanisms*, *Report of Expert Workshop* - University of Leuven, 2014, www.law.kuleuven.be/citip/en/news/item/coa-workshop-report.pdf.

[34] As pointed out by Ausloos, "the GDPR is first and foremost an instrument aimed at instilling responsibility, not control, nor liability. It is aimed at ensuring data is processed responsibly, which explains the centrality of the notion of fairness". J. Ausloos, *The Right to Erasure in EU Data Protection Law: From Individual Rights to Effective Protection*, Oxford, Oxford University Press, 2020.

can exercise the rights in practice"[35].

The concept of data controller is autonomous and functional. This means that it should be interpreted solely on the merit attributed to it by the EU legal framework (i.e. the GDPR) and it may be derived from a de facto analysis of the actual roles of the actors in place. It has been undergoing a rapid expansion in modern data-based environments and its broad interpretation[36] by recent case law has opened up accountability to multiple actors within the data collection and data processing chain. Namely, courts have highlighted the necessary broad definition of the concept of data controllers, as laid out by the Directive 95/46 superseded by the GDPR. The determination of the means and purposes of the processing can be found in specific parts of that processing. This led to an equally broad definition of joint controllership[37], necessary for the effective protection of data subjects.[38]

Data controllers are determined according to, and for each of the personal data processing operations. This articulation of actors is complexified when one considers distributed architectures, decentralised networks, and user-centric design. In all these technological systems, multiple actors are participating in the determination of the means and purposes of the personal data processing.

The application of these criteria is shifting based on the existing complex data processing realities. Even if the legislator has firmly repeated that determination over both the purposes and the means of the processing is critical in order for an entity to be qualified as a data controller, this corresponds less and less to the reality of personal data processing networks. Interpretations stemming from Article 29 Working Party's position, the recent opinion published by EDPB, and established case law are also distancing themselves from this strict interpretation. Namely, the first has already pointed out the primacy of the purposes over the means of the processing in the fact that the purposes are solely determined by the controllers while oftentimes the means are partially determined by data processors[39]. Similarly, the EDPB goes on to distinguish between essential and non-essential means of determination.[40]

European case law has leaned less on the distinction between essential and non-essential means of processing but has decisively created a broad frame of reference for the application of joint controllership[41]. In case of doubt when it comes to the determination of essential or non-essential means of the processing, the determination of a data controller will be defined by the entity that determines the purpose. In other words, decision power over merely technical and/or organizational means, may well be outsourced to a processor[42].

It is only when processors determine also essential means of the processing and/or they proceed to define (additional) purposes, that their processor status is superseded by that of controller. The precise tipping point of this transformation is still unclear from a normative point of view. For instance, it could be determined by assessing whether the processor serves solely the controller(s)'s

[35] Article 29 Working Party, Opinion 1/2010 on the concepts of controller and processor (WP 169) 00264/10/EN,1.

[36] As highlighted by case law, "in accordance with the aim pursued by Directive 95/46, namely to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data, Article 2(d) of that directive defines the concept of 'controller' broadly as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data". Thus, the broad interpretation of the concept of controllership, as supported by Courts, aims to ensure the necessary high level of protection of the fundamental right to data protection. See European Court of Justice, C-40/17, *Fashion ID GmbH & Co.KG vs Verbraucherzentrale NRW eV*, 29th July 2019, paragraph 65.

[37] "Joint responsibility of several actors for the same processing, does not require each of them to have access to the personal data concerned" See European Court of Justice, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, paragraph 69.

[38] See European Court of Justice, C-131/12, Google Spain, 13 May 2014, paragraph 34.

[39] This means that decision power over merely technical and/or organizational means, can be determined to a processor: see Article 29 Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*,00264/10/EN WP 169, 16 February 2010, 12.

[40] According to this distinction, "essential means are closely linked to the purpose and the scope of the processing and are traditionally and inherently reserved to the controller (…) Non-essential means concern more practical aspects of implementation, such as the choice for a particular type of hard or software or the detailed security measures which may be left to the processor to decide on." *Ibid*, p.14.

[41] See previous analysis on the broad interpretation of the concept of controllership.

[42]The European Court of Justice has repeatedly supported a wide definition of controllers, in order to meet the objective of effective and complete protection pursued by data protection law and in the light of the decisive role of the controller.

interests and follows their discretional power[43]. For every operation that a processor goes beyond the controller's directives, they would likely be considered controllers themselves.[44]

While the concept of joint controllership is not new[45], the GDPR has introduced relatively more concrete rules on how the relationship shall be governed. Case law[46] has developed standards of interpretation and provided clarifications on how responsibility and liability shall be allocated between different actors involved in the data processing.

The dynamic and functional nature of the (joint) controller concept requires a case-by-case analysis, taking into account the circumstances and the personal data in question. A series of recent decisions on a European level have led to the broadening of the concept of (joint) data controllership, for a "more complete protection of rights". Thus, this was an intentional shift in the CJEU in order to better accommodate data subjects in the modern and complex data ecosystem. While this objective-oriented broad interpretation of controllership laid out norms of finding accountable actors, it did not go further in describing the conditions of dividing responsibility and, at times, liability[47]. These interpretations have revealed uncertainties in the determination of liable actors. For instance, in the *Wirtschaftsakademie Schleswig-Holstein* case, the CJEU decided that "Directive 95/46 does not, where several operators are jointly responsible for the same processing, require each of them to have access to the personal data concerned".

Similarly, in a different case, the CJUE ruled that "a natural or legal person who exerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller".

Finally, this case law 'triptych' is completed with FashionID case, which pointed towards a 'phase-oriented' approach to data controllership. The Court pointed out that "the existence of joint liability does not necessarily imply equal responsibility of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, with the result that the level of liability of each of them must be assessed with regard to all the relevant circumstances of the particular case".

The Court's approach in addressing complex data processing ecosystems and dividing the responsibility of different actors based on their participation on specific phases in the processing, has been criticized for its lack of clarity as overachieving and underperforming[48]. According to some authors, the expansion of liability in that way "may thus deprive data subjects of effective protection, in particular where they lack knowledge of the specific purposes of third-party processing that they enable".[49] This is particularly problematic in the context of new user-centric technological architectures of data processing. For instance, decentralized architectures may "place data controllers in a contrary position as actors orchestrating or coordinating processing, but not actually seeing the data themselves".[50] As pointed out earlier, the CJEU has already highlighted that access to the data is not a necessary precondition to being allocated the role of a joint controller.

[43] Article 29 Working Party, Opinion 1/2010 on the Concepts of "Controller" and "Processor", 25.

[44] B. Van Alsenoy, *Allocating Responsibility among Controllers, Processors, and "Everything in between": The Definition of Actors and Roles in Directive 95/46/EC*, in *Computer Law & Security Review*, 2012, vol. 28, issue 1, 24-43.

[45] See the definition of controllers in the Directive 95/46/EC.

[46] See European Court of Justice, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* vs. *Wirtschaftsakademie*, C-210/16, 5 june 2018, *Tietosuojavaltuutettu vs. Jehovan todistajat - uskonnollinen yhdyskunta*, C-25/17, 10 July 2018 and *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*.
To be noted that while these judgments were issued by the European Court of Justice on the interpretation of the concept of joint controllers under Directive 95/46/CE, they remain valid in the context of the GDPR, given that the elements determining this concept under the GDPR remain the same as under the Directive.

[47] The recent guidelines from the E.D.P.B., aim to try to partially amend this ambiguity.

[48] See for instance R. Mahieu and J. van Hoboken, *Fashion-ID: Introducing a Phase-Oriented Approach to Data Protection?*, in *European Law Blog*, 2019.

[49] L. Edwards, M. Flinck, M. Veale and N. Zingales, *Data subjects as data controllers: a Fashion(able) concept?*, in *Internet Policy Review*, https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400.

[50] *Ibid.*

3.2. *Data controllers in decentralized identities*

The creation of a digital identity based on a decentralized, user centric (or self-sovereign), blockchain-based systems which stem from European institutions, is based on the principles of decentralization and sovereignty-institutional aspirations for the provision of services to all European citizens. However, it quickly becomes clear that these concepts are poorly defined both legally and technologically. If a distinction must be made between technological architectures promoting the centrality of the user for the provision of services and those promoting self-sovereignty, it is not obvious. Is it itself relevant? Similarly, both decentralization and people sovereignty are seen as the solution to combat the growing centralization of data in the hands of certain actors. However, nothing is less certain as long as power relations in any infrastructure remain subject to centralising forces and as long as each identified person needs the service to be provided through a specific network of actors in order to continue to access the desired services. In practice, it is difficult to imagine the disempowerment of the state as a provider of digital identity in favour of a (self-sovereign) decentralized identity. As part of its sovereign powers, the institutional responsibility to create and maintain identification technological structures is also ensuing (or at least– it should ensue) accountability to the corresponding actors.

The creation of decentralised infrastructures on a European level cannot be guided by a design principle to facilitate the removal of such accountability structures from responsible institutions, but it should maintain both security and accountability. In data protection terms, this would translate in the responsibilization of key actors in the identity system.

The allocation of obligations[51] between the different actors in distributed ledgers has been a point of contention the past years. Finck's work on GDPR compliance and blockchains presents the contrasts and uncertainties in the different shades and forms that distributed ledgers might appear, on a both technological and governance aspect. In her report for the European Parliament, Finck presents in detail how the existing European normative framework on data protection might apply on distributed ledgers, but more specifically, on public permissionless blockchains. She underlines that this lack of legal clarity on these decentralized architectures is "due to different understandings of what a blockchain is and how it is used, but also the different roles of various actors depending on the relevant technical and governance designs (such as what consensus protocols are used) and the uncertain legal test that ought to be applied".[52]

As the variations of the types of blockchains unfold, the designated actors that exercise significant influence on the means and purposes of the processing becomes blurred. For instance, in public permissioned blockchains, many different parties are involved in determining the means of the processing. This determination can be top down, from a company or a decisive entity, or it can stem from a consortium and any association of actors.

The determination of the means signifies, in the case of distributed ledgers, the decision-making power over the software architecture, the data centers constituting nodes, and the terms of the data processing. With respect to these permissioned blockchains and for the data processed on the distributed ledger, nodes are more likely to be qualified as data processors than as controllers. They are executing the necessary software to ensure consensus, but have little control over the determination of the means or the purposes of the processing. So, hired to perform the necessary computations, the nodes of a decentralised identity network would be considered as joint controllers on the personal data stored in the distributed database that constitutes the ledger, only if they have the power to arguably determine the essential means of the processing. Ultimately, their responsibility and ability to (jointly) participate in making substantial decisions related to the organisation of data processing architectures such as "what data to process and for how long, which third parties have access to the data, when and how data can be

[51] For the allocation of responsibilities and liabilities between different entities according to the normative framework, see B. Van Alsenoy, *Data protection law in the EU: roles, responsibilities and liability*.

[52] M. Finck, *Blockchain Regulation and Governance in Europe*, Cambridge, Cambridge University Press, 2018, 43.

manipulated"[53] would have to be de facto assessed.

This non-binding guidance issued by the Article 29 Working Party, the predecessor to the forthcoming interpretation by the EDPB, mentions these examples as an indication to what the determination of essential means would imply for a data controller in contrast to the obligations of the data processors. Furthering this argumentation with regard to a decentralised digital identity system, the institutional support for the creation of the blockchain-based system is justifying the assessment over the possible qualification of responsible actors among European or Member State institutions. For instance, it could be examined if these institutions, which knowingly enable the personal data to be processed on the ledger –designed with the participation of a third party or in-house– can be qualified as data controllers based on the case law that sees joint controllership when there are converging decisions between the two entities in question.[54]

On a European level, and taking into account the aforementioned CJEU judgment in Jehovah's Witnesses in combination with the eIDAS revision that creates the space for new blockchain-based identity systems to be created, the role and accountability of European institutions is put in question. Blockchain-based systems developed and provided by the European Commission under a mandate to deliver EU-wide, cross-border public services, oftentimes follows a GDPR actor qualification logic. The creation and support of this identification system seeks to support the objectives of the EU Single Market. Taking these elements in consideration, it is easy to consider European institutional bodies as having "organised, coordinated and encouraged" the processing of personal data on chain and that they shall be considered as joint data controllers.

4. *The aspiration of user control: the data subject as a data controller*

The focus on creating user-centric data processing operations has brought up the question on the responsibility of each user as a joint controller. If users are responsible and in the center of decision-making on personal data processing operations, what is their liability and legal responsibility?

The privacy protective architectures such as personal data stores (PDSs), or –in the examined case– the end-user digital identity wallets are some examples that illustrate the central role of users. Practically, this means that the data in question are not being held and processed in a centralized manner on the cloud, but rather they are held in a decentralized manner by data subjects themselves[55].

Decentralized identity architectures rely on the premise that end users/data subjects will be in full control of their data. In practice, the design of such a system that gives full control of the personal data to the end user, creates a level of responsibility as data controllers for the data that will be stored in their wallets, collected through the use of the applications that are onboarded on top of the distributed ledger. So, end users will be able to store personal data related to themselves and in that manner, they will be qualified as data controllers jointly with other participating entities that define and enable the means and purposes of the processing on the network.

The application of the household exemption does not appear to be applicable in the cases of user wallets. According to article 2(c) GDPR, "this Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity". This exemption, designed to protect individual users processing personal data within the context of a personal household from the responsibility of controllership, is to be narrowly interpreted. The CJEU[56] has highlighted this narrow interpretation of the exemption in order to ensure the safeguard and efficient protection of data protection principles. There are additional criteria to this interpretation: that personal data in question cannot be shared

[53] Article 29 Working Party, *Opinion 1/2010 on the Concepts of "Controller" and "Processor"*.

[54] In the *Jehovah's Witnesses case*, the CJEU determined that the religious community is a data controller, jointly with its members who exercise the collection and the personal data processing during door-to-door preaching. The community participated in the determination of purposes and means by organizing and coordinating the activities of its members, which helped to achieve the objective of the Jehovah's Witnesses community.

[55] L. Edwards, M. Flinck, M. Veale and N. Zingales, *Data subjects as data controllers: a Fashion(able) concept?*

[56] European Court of Justice, *Lindqvist*, C-101/01, 6th November 2003.

with an indefinite number of people and the processing must not be 'directed outwards from the private setting of the person processing the data'[57]. Cumulatively, it appears that this exemption would not be able to be applied to users who use the data stored in their user wallet application for the purposes of aggregating and seeking external services. Thus, the purpose of the wallet is to efficiently store personal data, but with the aim to have that data interact selectively (depending on the wishes of the user in question) with external providers. The household exemption could not be applicable in those circumstances.

Finally, the open question that remains is whether this architecture leaves room for personal data being stored in an end user's wallet, but also referring to a third data subject. Whether that is a possibility or not in technical terms, this could lead to the qualification of the user whose wallet is being used to store that third party data as a joint controller together with the entities, third actors, platforms, applications, that enabled the collection and processing of the personal data that ended in the wallet of the end user. This qualification exposes users to a set of overbearing obligations towards other data subjects[58].

The qualification of the data subject as a data controller is still contested to this day, because of the paradox that it creates. Namely, and as succinctly described by Van Alsenoy, "there are essentially two arguments which can be made against such a proposition. First, this interpretation cannot be reconciled with the regulatory scheme of EU data protection law. This scheme is predicated on the notion that the data controller is an entity other than the data subject him– or herself. An individual person might act as a controller of personal data relating to others, but not of his or her own personal data. Accepting that the data subject could act as a controller of the processing of his own personal data would have rather absurd implications: the data subject would have to obtain consent from him– or herself, provide him– or herself with notice, etc. Second, the fact that the data subject authorizes the disclosure of personal information within a certain context merely signifies his or her agreement towards processing. It does not exclude the presence of another entity who determines the "purposes and means" for the processing of these data. Even where the individual has the ability to "control" the release of his or her personal data (and might even decide the medium that is used), this does not alter the role of the collectors or handlers of the individual's data[59].

5. *Conclusion*

Digital identity is a key element in information value chains. For this reason, the impact of the identity infrastructures built on a European level needs to be considered and the system designed accordingly. Digital identity has evolved into a digital artefact, a technological solution aspiring to formalize the individualization of access to computer networks, and to address the challenges present throughout this process.

In this context, the place of the person will have to be questioned. If the implementation of a decentralized identity involves the use of technical architectures that are created on consensus-based standards and qualified actors who have proven their expertise, the accountability should follow the same logic too and not that of user centricity or of self-sovereignty. If this is the case, the notion of informational self-determination should be prioritized as a guiding principle, one which will also be reflected in the accountability regime.

Decentralized identity infrastructures indeed present the risk of increased accountability of individual citizens and a correlative disempowerment of other actors involved, including public ones. However, this responsibility must give way because without this, the logic of placing the individual at the heart of the decision-making process will result in the birth of an obvious imbalance between the various actors, to the detriment, paradoxically, of the person concerned.

The emphasis put in decentralizing the technical system of digital identity production, expression, and validation, is but only one part of the process of claiming back control over our understanding of selective self-revelations vis-à-vis the state. Legal compliance,

[57] European Court of Justice, *FrantišekRyneš v Úřad pro ochranuosobníchúdajů*, C-12/13, 11 December 2014, paragraph 33.

[58] See B. Van Alsenoy, *Data protection law in the EU: roles, responsibilities and liability*.

[59] B. Van Alsenoy, *Data protection law in the EU: roles, responsibilities and liability*, paragraph 700.

especially in data protection terms, might ask the relevant questions on how personal data flows within the relevant identity systems, but it is not sufficient to address foundational issues on the necessity in permanent identification, the contexts and limits of revealing parts of our identity, the discrimination. This is why clear accountability structures –especially for European-wide systems, are essential.

Admittedly, the role of the state is polyvalent in identity creation, validation, authentication, and management systems. Exercising its sovereign power in (legal) identity creation, validation, and authentication, the state is also engaging in a rather complex network of relationships and data flows under any of the capacities: in the performance of e-government services, in the cross-border digital identification of its citizens, in the collaboration between the public and the private sector for infrastructural support and creation of digital identity management systems. The State, guarantor of civil (digital) identity[60], has a formal responsibility to ensure the conditions of private company involvement in the digital identity infrastructure provision. This exercise can be guided by fundamental rights such as (but not limited to) the right to data protection, the right to privacy, the right to non-discrimination, etc.

As this article has shown, decentralized technological designs are a pragmatic approach towards the enabling and stimulating of user control. Within this technological design, data protection and privacy become technological affordances that materialize as a visible characteristic of the identity provision service delivered to the end user. While this is a laudable goal, it cannot come at the expense of distancing the formal guarantor of the provision of identity, ie the State (and the corresponding European institutions) from its accountability obligations and its role as data controller in many identity provision services.

[60] Y. Poullet, *L'identité numérique en quête de son identité juridique*, in J. Eynard, (ed.), *L'identité numérique. Quelle définition pour quelle protection?*, Bruxelles, Larcier, 2020, 193-206.