European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 171-184
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 14

*GDPR and Blockchain Technology in the New Multifaceted Scenario of Health Data Protection: Overcoming the Tensions Between Technology and Law**

Rolando Poggi
(PhD Candidate in Labour, Development and Innovation at University of Modena and Reggio Emilia and Member of Marco Biagi Foundation's Privacy Observatory)

ABSTRACT The EU General Data Protection Regulation n. 679/2016 (GDPR) stands as an element of support for the development of the digital economy. Among the many facets of society and areas of the economy that it influences, the GDPR also impacts on scientific research that uses personal data. The paper addresses the most important aspects of the GDPR that are relevant for the purposes of data protection in health research. Then, the study leverages the points of contrast between the "train of innovation" on which the new Distributed Ledger Technologies (DLTs; of which blockchain is the most celebrated example) travel at full speed and the rules contained in the GDPR. And indeed, despite the many tensions between the two actors (e.g., right to be forgotten, data controllership etc.) blockchain technology could be significantly propaedeutic for health research and for healthcare as a whole, and it could even reflect its advantages on the very culture of privacy regulation, by making data-protection mechanisms more efficient and by improving transparency in GDPR compliance paradigms. As a key to understanding, the paper uses one of the guiding principles of the GDPR: that of not hindering, but rather supporting technological progress. For this reason, blockchain will be deeply examined in its most relevant characteristics to investigate its extensive potential and, before that, its laborious compatibility with the legal requirements of the European regulation on privacy and with the main interpretative contributions from Europe's regulatory Authorities and Courts.

1. *Introduction: the complex scenario of privacy regulation in modern healthcare*

Data has become a milestone of economic and scientific development. In this context, data-protection legislation is constantly evolving: new contents and forms are emerging, and they require specific and diversified interventions by legislators. In *the broad horizons opened by new technologies, adequate measures are needed to protect personal data as well as a balanced regulation, capable of weighing opposing interests.

It is therefore essential to analyze in an interdisciplinary perspective the impact of the use and circulation of data and of disruptive emerging technologies on the main rules for data protection in human activities.

The implementation of the GDPR draws attention to issues that are important for the kind of scientific research that uses personal data. It was found that "an adequate analysis of health-related Big Data can help predict epidemics, treatments and diseases, as well as improve the quality of life and avoid preventable deaths".[1]

The need to manage patients' personal-health data correctly and appropriately has emerged with great evidence from the recent COVID-19 outbreak. The pandemic has confirmed (in a very harsh and urgent manner) that the use of patient data can be crucial for scientific research. In recent years, in the health sector (as in many other sectors) a considerable amount of data has been collected.[2] This aspect and the increase in the

*Article submitted to double blind peer review.

[1] "Proper analytics of big healthcare data can help predict epidemics, cures, and diseases, as well as improve quality of life and avoid preventable death", I.A.T. Hashem, V. Chang and N.B. Anuar, *The role of big data in smart city*, in *International Journal of Information Management (IJIM)*, vol. 36, 2016, 748; in this regard, see also A. Pentland, T. G. Reid and T. Heibeck, *Big Data and Health: Revolutionizing medicine and Public Health - Report of the Big Data and Health Working Group*, presented at World Innovation Summit for Health, Doha, 10-11 December 2013, 2.

[2] The availability of data will grow more and more, also as a result of new data sources such as sensors, social networks, mobile devices, (Internet of Things) being introduced into the social and economic spheres. E. Mor-

world population have led to new forms of health treatments and services.[3] And indeed, healthcare institutions currently experience an increased demand of real-world data from industry and research organizations, so much so that people started using the expression "Healthcare 4.0"[4] to refer to today's high degree of interconnection and sharing of data between patients, doctors, and healthcare facilities.[5] In this scenario, unauthorized sharing, and highly publicized breaches and robbery of sensitive data avidly erode the trust that people lay in healthcare institutions.[6] This is certainly a situation that commands rethinking and consideration of alternative approaches. Tools such as the groundbreaking blockchain technology, as well as systems based on artificial intelligence (AI), present great potential in this perspective.[7] According to Elisa Ficarra, AI is at a state of development such that it can offer technologies capable of modeling the complexity of medicine".[8] On the other hand, the use of new and disruptive technologies in the health domain can also result in pitfalls: complex and unusual ethical problems concerning the care and treatment of patients, risks related to the possibility that someone will hack the systems, as well as critical profiles in terms of protection of the data collected. Hence the need for interventions by the legislator with the aim of regulating these aspects in a way that is more adherent to day-to-day concrete experiences. In this regard, it seems worth to recall the issue of tangible and intangible infrastructures, which must allow, as the European Parliament has affirmed, equal access for all citizens to these innovations, tools, and technological interventions.[9]

1.1. *Genetic data*

In the present paper, the focus is on the protection of personal data in health research. In such a context, therefore, we are dealing with genetic data.

The study of genetic data is of great importance not only for the subject to which the data refer, but for the community as a whole. And indeed, now more than ever, a significant degree of interest can be found in sharing information for research purposes.

We can identify two opposing sides of genetic data. On the one hand, they constitute a very precious resource for the development of science among humans: it is indeed possible, by studying genetic information, to deepen the knowledge of pathologies and consequently predict the onset of diseases and ensure the possibility of intervening in advance on them; on the other hand, however, it is a particular category of personal data that plunges into the most intimate sphere of the people.

This polymorphic nature becomes even more evident if we take a quick look at some

ley-Fletcher, *Digital healthcare: new scenarios and new professions*, in *Astrid Rassegna*, vol. 18, 2016, 1.

[3] In this connection R. Ducato, *Database genetici, biobanche e "health information technology"*, G. Pascuzzi (ed.), in *Il diritto dell'era digitale*, Il Mulino, Bologna, 2016, 305-320.

[4] On this topic, P. Jayaraman, A.R.M. Forkan and A. Morshed, *Healthcare 4.0: A review of frontiers in digital health*, in *WIREs Data Mining and Knowledge Discovery*, vol. 10, 2019, 1-23; see also J.J. Hathaliya and S. Tanwar, *An exhaustive survey on security and privacy issues in Healthcare 4.0*, in *Computer Communications*, vol. 153, 2020, 311-335.

[5] E. Coiera, *Guide to Health Informatics*, Sydney, CRC Press, 2015. See also J. Hathaliya, P. Sharma and S. Tanwar, *Blockchain-based Remote Patient Monitoring in Healthcare 4.0*, presented at 2019 *IEEE International Conference on Advanced Computing, IEEE (Institute of Electrical and Electronics Engineers)*, 13-14 December 2019, especially 87.

[6] A. Hasselgren, K. Kralevska and D. Gligoroski, *Blockchain in healthcare and health sciences - A scoping review*, in *International Journal of Medical Informatics*, vol. 134, 2020, 4.

[7] It has been noted that the use of artificial intelligence "understood as the massive and targeted use of algorithms and of data analysis techniques to guide the behavior of human beings with the declared purpose of preventing disease, is playing an increasingly important role, connected but different from the search for new forms of therapy, new medicines, new treatment technologies". R. Bifulco, *Intelligenza Artificiale, internet e ordine spontaneo*, in F. Pizzetti (ed.), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Turin, Giappichelli, 2018, 383 ff., especially 386; see also A. Spina, *La medicina degli algoritmi: Intelligenza Artificiale, medicina digitale e regolazione dei dati personali*, in F. Pizzetti (ed), *Intelligenza Artificiale*, 319 ff.

[8] E. Ficarra, interview in the context of FocusUnimore newsletter article *Dati sanitari: anche una docente Unimore nel gruppo di lavoro dell'Healthcare Data Innovation Council, al servizio della Comunità Europea*, in FocusUnimore, July 2022, n.28, available at www.focus.unimore.it/luglio-2022.

[9] European Parliament, *Resolution of 16 February 2017 on improving the functioning of the European Union building on the potential of the Lisbon Treaty*, Strasbourg, Point 40, where the Parliament asks the Commission and the Member States to promote the development of assisted technologies in order to favor the development and adoption of these technologies by subjects who need it, in accordance with art. 4 of the UN Convention on the Rights of Persons with Disabilities, which the Union has signed.

legal sources: the principle of benefit-sharing, affirmed by the UNESCO Declaration on the Human Genome,[10] and the right to free scientific research, already affirmed by articles 9 and 33 of the Italian Constitution and most recently reaffirmed at the UN[11] would seem to imply a *favor* for a freer use of genetic data rather than for an enforcement of the stringent regulations on privacy protection, which impose significant precautions on health facilities and laboratories for the use of this peculiar type of data in research. The discipline relating to the protection of this category of data, in fact, "stands at the intersection between the protection of health, the freedom of research and scientific experimentation, and public safety, creating situations whose regulation requires complex operations balancing".[12]

Art. 9, par. 1 of the GDPR inserts genetic data (together with biometric data) among the "special categories of personal data" (the so-called "sensitive data") whose processing is prohibited, with the exceptions identified in the following paragraph. Genetic data (as well as biometric data) then became, on a legal level, a species of the sensitive data *genus*, so much so, as it is known, that it can be considered "super-sensitive" data.[13]

1.2. *Anonymization*

In the kind of research that involves the use of biobanks, the protection of the data subject (understood as the natural person who has provided human biological material) consists in protecting sensitive personal information by ensuring that, when processed, it is in fact impossible to identify the individual to whom those data refer. Such task is generally addressed by resorting to anonymization and pseudonymization procedures. However, it is now known that anonymization is often a partially reversible process. And indeed, anonymization usually consists in the loss of some attributes connoting the personal data, so that the latter no longer consists of information attributable to a subject. This elimination, however, is not always such as to totally exclude re-identification: data can undergo procedures that allow to re-identify the subjects to which they refer. Studies were made in this regard, and they have shown the possibility of re-identifying anonymized data sets.[14] These aspects have built a new vision of the relationship between personal data and anonymous data that is no longer binary, but rather a perspective that ranks these two types of data at the ends of a graduated scale where variability is given by how easy it is to re-identify the data.

1.3. *Data breach*

It should be emphasized that health databases possess peculiar traits: a large-scale health database is not just an up-scaled version of a normal data collection: indeed, biobanks generally bring together much larger and much more diverse sets of information and biological materials and, above all, the data present in a biobank bear a significantly higher value.[15]

[10] UNESCO, *Universal Declaration on the Human Genome and Human Rights*, adopted by UNESCO General Conference on November 11, 1997.

[11] The right to science and scientific progress as a human right has had a recent and decisive recognition at the UN, with the consequent burden on States to implement the tools for its implementation and protection. See United Nations Organization, Committee on Economic, Social and Cultural Rights, *General comment* n. 25 of 30, New York, April 2020, 6-7.

[12] A. Iannuzzi and F. Filosa, *Il trattamento dei dati genetici e biometrici*, in S. Scagliarini (ed.), *Il "nuovo" codice in materia di protezione dei dati personali*, Modena, Giappichelli, 2019, 116.

[13] These normative clarifications are very important because, prior to the entry into force of the GDPR, genetic data was an ill-placed concept. The notion of genetic data was formally extraneous to that of sensitive data, for they did not figure in their legal definition. And indeed, Directive 95/46/EC, relating to the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data (also known as the "mother directive"), did not recognize the specificity of genetic and biometric data and it therefore made them fall into the general category of personal data, that included "any information relating to an identified or identifiable natural person ("data subject")".

[14] According to the findings of the first Permanent Ethics Committee of the United States, as early as the late 1990s, the samples which were identified at the time of collection, even if subsequently coded or anonymized, inevitably maintained a certain level of re-identifiability. In this regard, see also S.N. Eshun and P. Palmieri, *Two de-anonymization attacks on real-world location data based on a hidden Markov model*, presented at *2022 IEEE European Symposium on Security and Privacy Workshops*, Genoa, 6-10 June 2022, 1-9.

[15] The value of Big Data, understood according to Doug Laney's paradigm of the "five v's" (volume, variety, velocity, value and veracity) could be the most important "v". There are those who point out that "the data [themselves are] the main object of entrepreneurial activity. The data (both personal and anonymous) [are] captured, conveyed, processed and for the most part stored and accumulated, representing a different and alternative form of 'capital' to the surplus value obtained from the sale of services or advertising space". G. Giannone Codiglione, *Libertà d'impresa, concorrenza e neutralità*

And indeed, it is precisely the considerable value of health-related data that has attracted the attention of numerous computer hackers who have been targeting patient data collections stored (in a more or less secure manner) in the archives of health facilities, thus configuring examples of the phenomenon known as data breach.[16]

It seems that, contrary to what one might expect, the attackers are not only eager to get hold of credit cards. In fact, more and more violations appear rather as preparatory acts for a different and more complex "criminal design": that of identity theft. Using spear phishing strategies, often by means of ransomware,[17] hackers ask for large sums of money in exchange for the medical records they hold hostage. Medical records are in fact a much more valuable "asset" than credit card data.[18] Indeed, if the latter end up in the wrong hands, they can easily and quicky be deprived of their effectiveness at the request of the owner; but the offense that moves through the medical records and health information of patients is more complex and insidious.

Such a scenario raises a lot of concerns, so much so that one wonders if it is possible to find new systems to collect and store data that would prove a more resistant solution not only to cyber-attacks (be them malicious or accidental) but also to the concrete risk of reversibility of the traditional anonymization procedures. Blockchain technology seems to have considerable potential precisely in these aspects.[19]

2. *The advent of Distributed Ledger Technologies (DLTs): characteristics of Blockchain*

Let's clarify the features of blockchain that are relevant to this analysis, in order to understand why this class of technologies promises a revolutionary innovation in the healthcare domain.[20]

First, it should be stressed that Blockchain is a particularly complex technology, aimed at carrying out various operations including transactions management and value exchange. It can be synthetically represented as a database that is distributed[21] among the users

della rete nel mercato transnazionale dei dati personali, in *Diritto dell'informazione e dell'informatica*, 2015, 911. See also D. Laney, *3D Data Management: Controlling Data Volume, Velocity, and Variety*, Stamford, CT, in *Gartner*, file 949, February 2001.

[16] Are data breaches frequent? 2019's Annual Report of the Italian data protection authority outlines noteworthy information in this regard: the panel chaired by Antonello Soro informs us that in 2019, in Italy, the Authority received as many as 1443 reports of IT incidents concerning personal data: this translates to nearly four data breaches per day. Only one year earlier, in 2018, 650 attacks had been registered (interestingly, of these 650 reports, 630 had occurred after 25 May, i.e., the date of entry into force of the GDPR which made reporting data breaches mandatory). See Garante per la protezione dei dati personali, *Annual report 2019*, Rome, 23 June 2020.

[17] The term "ransomware" refers to a class of malware (computer viruses) that makes the data on the infected computers inaccessible and asks for the payment of a sum of money (usually via *bitcoin*, *ethereum* or other cryptocurrency payment method, with the aim of rendering the transaction untraceable) to have them back.

[18] Ponemon Institute's 2016 Annual Report efficiently illustrates the data-breach scenario in the medical sector, outlining that data breaches in healthcare are increasingly costly and frequent, and continue to put patient data at risk. Based on the results of this study, it is estimated that data breaches cost the healthcare industry $6.2 billion, and during the two-year span before the report the average cost of a data breach for healthcare organizations was estimated to be more than $2.2 million. "No healthcare organization, regardless of size, is immune from data breach". Ponemon Institute, *Benchmark Study on Privacy & Security of Healthcare Data* (Annual Report 2016), 1.

[19] On the usefulness of blockchains from a health-data breach perspective, see Vv.Aa., *Blockchain: Opportunities for Health Care*, Deloitte, August 2016, 6: "An interoperable blockchain can strengthen data integrity while better protecting patients' digital identities […] Each participant connected to the blockchain network has a secret private key and a public key that acts as an openly visible identifier. The pair is cryptographically linked such that identification is possible in only one direction using the private key. As such, one must have the private key in order to unlock a participant's identity to uncover what information on the blockchain is relevant to their profile. Therefore, the blockchain public/private key encryption scheme creates identity permission layers to allow patients to share distinct identity attributes with specific health care organizations within the health care ecosystem on as-needed-basis, reducing vulnerabilities […] on all sides and allowing for data access time limits to be introduced by patients or providers"; on the usefulness of blockchain for anonymization, see F.J. De Haro-Olmo, A.J. Varela-Vaca and J.A. Álvarez-Bermejo, *Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review*, in *Sensors*, vol. 20, issue 24, 2020, 7171.

[20] In this connection, Vv.Aa., *Blockchain: Opportunities for Health Care, Deloitte*, August 2016, especially 5.

[21] The distribution of a database among the users of an installment represents the distinctive feature of the so-called distributed ledger technologies (DLTs), of which the blockchain is the most famous example. The concept of distributed ledger is opposed to the traditional logic of centralized data management (for example, financial institutions, public bodies, health research structures, etc.), subject to the control of one single and superordinate central authority. In DLTs there is no hierarchical order: all network users are at the same level and can only act with the consent of the majority.

of a network.[22] More specifically, blockchain consists of a public and shared ledger capable of automatically update on each node[23] participating in the network. This ledger is structured in blocks, each of which represents a number of transactions whose origin and time of execution are indelibly and immutably set through an asymmetric key-encryption mechanism and a timestamp. Each block is irreversibly linked to the previous one through a particular logarithmic operation, the so-called hash function,[24] and forms the chain of blocks.

It must be emphasized that, in principle, there is no such thing as "the" blockchain. It is in fact a class of technologies that have different technical properties and different rules. In this analysis, when the expressions "blockchain(s)" and "blockchain technology" are used, they refer to a class of technologies that can take many possible different forms, but generally share a few general principles. Therefore, when trying to determine if a specific blockchain, used in a specific context, is compliant with the GDPR, it is nonetheless necessary to investigate the precise characteristics of that blockchain, used in the specific case.

2.1. *The health sector*

In recent years, blockchain technology has become very trendy and has penetrated different domains, mostly due to the popularity of cryptocurrencies. A sector in which blockchain technology has a significant potential in terms of data protection is that of healthcare, to the extent that the data used in this field (genetic data), as we have seen, possess characteristics that distinguishes them from any other type of data. Furthermore, healthcare is a field where the ability to connect many different systems quickly and safely is of central importance, not to mention the need for great accuracy in the preparation and management of electronic healthcare records (EHR). In the health domain, to both maintain the patients' privacy and exchange data with other institutions in the healthcare ecosystem, access control, provenance, data integrity and interoperability are indeed crucial.

2.2. *Decentralization, disintermediation, immutability*

There are two main reasons why blockchain is being touted as a groundbreaking conception that will fundamentally change many sectors and perhaps the entire economy. First, blockchain is based on the principles of decentralization and disintermediation. This means that blockchain allows for the exchange of data in an environment that is devoid of a superordinate "governor"; and in a direct manner, i.e., without the need for an intermediary. Decentralization and disintermediation have made blockchain the technology of choice for creating cryptocurrencies. Cryptocurrencies allow for the direct transfer of value from person to person by bypassing traditional intermediaries such as banks and, in doing so, disrupt the traditional financial system and the financial industry.

Second, the technology behind blockchain provides near-absolute reliability, anonymity, and immutability of the data records. Participants in blockchain transactions do not have to know or trust each other to take part in a transaction. Instead, participants rely on encryption and block-immutability to protect their data and to secure themselves from counterparty pitfalls. The data inside the blocks are accessible only to those in possession of cryptographic keys and, in the case of blockchain without authorization (*private and permissioned*, as will be seen shortly), the immutability of the data is guaranteed by the fact that it is necessary to obtain consent from all the participants not only to add new blocks to the chain, but also to remove them (and we will also see that

[22] See L. Parola, P. Merati and G. Gavotti, *Blockchain e smart contract: questioni giuridiche aperte*, in *I Contratti*, issue 6, 2018, 681 and seq.

[23] In information technology and telecommunications, a node is any hardware device capable of communicating with the other devices that are part of the system; it can be a computer, a printer, a fax machine, a modem, etc. In blockchain's specific context, a node is a computer connected to the blockchain network that stores a copy of the public ledger.

[24] The hash function transforms data of arbitrary length (i.e., a message) into a fixed-sized binary string called a hash. In blockchains, each block is identified with a hash which, through an alphanumeric string of a given length, summarizes and encodes the information relating to the transactions it contains. When adding a new block to the chain (containing new transactions originating from those contained in the previous block), the hash function will have as its object the information relating to the new transactions together with the identifying hash of the previous block. Basically, each new hash will also enclose the hash of the previous block, thus creating an indissoluble chain.

erasure and even "mere" modification of blockchain data represents a particularly laborious operation). Data ledgers in the blockchain can be suitable to store any type of information, so the technology can be used for nearly any kind of data-processing purpose.[25]

2.3. *The "resilience by replication" principle and the append-only nature of blockchain*

So, in essence, blockchain is a shared and synchronized digital database: therefore, it is essentially a database that does not exist in one place only, rather, it exists in parallel on many different computers and all these computers share the complete copy of the entire dataset present on the database. Those computers can be in many different places and, consequently, many different jurisdictions, which brings with it many legal issues. Blockchain precisely intends to pursue the resilience of the information contained in it through its replication, i.e., by replicating and storing data on many different servers. The idea is that even if some of those computers stop working, suffer malfunctions, or are destroyed, it is still possible to keep the database as such, as it exists in many different places.[26]

Another very important feature of the blockchain, especially from a GDPR perspective, is that it is an append-only database: a database in which one can only store data, because destruction or alteration of the data happens only in extraordinary circumstances and moreover, is very difficult to achieve. Another interesting feature of this class of technologies is the use of timestamps that contain a mechanism to track who carried out an operation and at what exact time.

2.4. *Public and private blockchains*

Blockchains are essentially divided into three categories. First of all, there are *public and permissionless* blockchains and there are *private and permissioned* blockchains. Basically, the difference is that public blockchains contain data (in most cases, encrypted or hashed) that are visible to all who want to access it; in the private blockchain, however, this is not the case. The difference lies in the fact that, in order to enter the network and add data to it, in the public type of blockchain it is not necessary to obtain the permission of anyone to do so, whilst in the permissioned-systems there is generally a central and superintendent subject (the so-called gatekeeper), who decides which parties can join the blockchain ledgers. Then, a third type of blockchain exists, and it is a *tertium genus* that sits halfway between the first two aforementioned types: it is in fact called *public-permissioned*, also known as *consortium*. Consortium-type blockchains allow only a selected group of nodes to participate in the distributed consensus process.[27] When a consortium-blockchain is established within a sector (for example, the healthcare, financial or insurance sector), it is opened for limited public use, which is partially centralized. Moreover, even for a consortium between organizations (for example, healthcare facilities, financial companies, government institutions) open for public use, it is still necessary to maintain trust mechanisms with a certain degree of centralization. It has been reported that the consortium-type blockchain appears to be the preferred design choice for health facilities.[28] And indeed, since healthcare-information systems deal with highly sensitive data, (which usually imply that a small number of entities should have access to them) a consortium blockchain may be more appropriate than an unauthorized public one to ensure that data are not accessible by those who have no rights to view them, while maintaining an appropriate degree of publicity motivated by public interest in research and

[25] For example, blockchains can be used as a good tool for identity management purposes. See K. Shraddha, *Building-Blocks of a Data Protection Revolution - The Uneasy Case for Blockchain Technology to Secure Privacy and Identity*, in *MIPLC Studies* (Munich Intellectual Property Law Center), vol. 35, 2018, 31-33.

[26] On this topic, see N. Al Azmi, G. Sweis and R. Sweis, *Exploring Implementation of Blockchain for the Supply Chain Resilience and Sustainability of the Construction Industry in Saudi Arabia*, in *Sustainability*, vol. 14, 2022; G. Li and J. Xue, N. Li, *Blockchain-supported business model design, supply chain resilience, and firm performance*, in *Transportation Research Part E: Logistics and Transportation Review*, vol. 163, July 2022.

[27] Z. Zheng, S. Xie and H. Dai, *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*, presented at 2017 IEEE International Big Data Congress, IEEE, Boston, MA, 11-14 December 2017, 557-564; M. Hölbl, M. Kompara and A. Kamišalić, *A Systematic Review of the Use of Blockchain in Healthcare,* in *Simmetry*, vol. 10, 2018, 470.

[28] A. Hasselgren, K. Kralevska and D. Gligoroski, *Blockchain in healthcare and health sciences - A scoping review*, 7; on this topic, see also E. Coiera, *Guide to Health Informatics*, Sydney, CRC Press, 2015.

the progress of medical science.

3. *Antinomies between Blockchain and GDPR: centralization vs decentralization; mutability vs immutability; data minimization*

Is there a way to reconcile the potential of blockchain technology with privacy regulation? How could blockchains be used in a way that is compliant with the GDPR?

An effective way to approach these questions is the following: instead of focusing immediately on how to force blockchains within the scope of the GDPR, one could analyze the GDPR using the blockchain as a key to understanding and, therefore, learning many interesting things on the GDPR itself. The first element that emerges from a reading of this type is a strong tension between the two players at stake: the GDPR and blockchains.

There are two general reasons why this tension, that has caused much controversy amongst media, scholars and even regulators, exists. First, as mentioned, blockchains generally decentralize data on different computers and this in turn decentralizes the governance of the blockchain. There are some implicit assumptions in the legal framework of the GDPR: one of these is that there will generally be one legal entity responsible for a specific set of data; this is, generally, not the case when using blockchains.

The second general tension that lies between this technology and the GDPR corresponds to the contrast between the mutability required by the GDPR and immutability, a fundamental characteristic of the blockchain. And indeed, the GDPR contains the obligation to change or delete data when the data subject requests for it. The problem is now the following: usually, blockchains are specially-designed to make said operation impossible or at least very difficult. That tension is manifested across different points of the GDPR.

One of the fundamental principles of the GDPR is the so-called *data minimization principle*: art. 5, par. 1 letter c) states that personal data are adequate, relevant, and limited to what is necessary with respect to the purposes for which they are processed. The idea is that you need to minimize the data you are using in a specific context. And there are two reasons this is difficult to achieve in a blockchain environment. The first reason is that the databases of a blockchain are continuously growing and, essentially, no data can be deleted;[29] the second reason concerns the aforementioned paradigm of resilience by replication: not only do data keep growing, but said data are also being replicated on many different computers, thus giving rise to copies of data everywhere.

Similar tensions can be identified when observing the purpose limitation principle pursuant to art. 5, par 1, letter b) of the Regulation: this tells us that personal data must be collected for certain explicit and limited purposes and cannot be further processed in a way that is incompatible with those purposes. Now, the addition of data to blockchain often serves a specific purpose, such as a transaction. But this is just the initial purpose. What happens next is that the data continues to be stored in the blockchain, and it is known that even data retention alone qualifies as data processing from a GDPR perspective.[30] Therefore, the question arising is whether from a GDPR-perspective it could be argued that not only the initial purpose of the transaction, but also the secondary use (represented by the "maintenance" of data) constitutes data processing. The answer to this question is not entirely clear as the notion of purpose limitation has not yet been interpreted in a way that is adequately corresponding to the blockchain dynamics.

3.1. *Right to erasure*

Then, there is the tension that has gotten the most attention so far. It is the obligation pursuant to art. 17 GDPR, which requires the deletion of data in certain circumstances;[31] it

[29] For this characteristic, as already mentioned, blockchains are usually described as an "append-only database": a database where, essentially, you can only add data, which will remain permanently stored.

[30] Not to even mention that further processing would also take place each time the network reaches the conditions for new data to be added.

[31] The circumstances in which the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay are the following:

(1) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(2) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
(3) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate

is the right to erasure, also known as the *right to be forgotten*. Art. 17 GDPR states that the data subject has the right to obtain from the controller the erasure of personal data concerning them without undue delay. Now, to determine whether the obligation of Article 17 can actually be met in a blockchain environment depends significantly on how the term "erasure" is to be interpreted from a GDPR perspective.[32] Therefore, on the one hand, it could be argued that erasure (which is neither defined in the Recitals nor in the legislative text of the GDPR) is to be interpreted with its literal meaning. However, this does not appear if you look at the Google Spain ruling of 2014:[33] in this judgment, the issue was not about deleting data, but about disconnecting search results from Google's search algorithm. Therefore, this judgment could be interpreted as meaning that there are situations in which a true erasure (in the sense of a total cancellation) of data is not necessary in order to fulfill the obligation of art. 17, as this was not in dispute within this judgment. And indeed, the Court of Justice ruled that European citizens have a right to request that commercial search engines, such as Google, should remove links to private information when asked, provided the information is no longer relevant.

Moreover, when looking at what the various data-protection Authorities have stated on this issue, it appears that there is no agreement between them on how to interpret the term "erasure". The British ICO, for example, has been arguing for several years now that putting data "beyond use"[34] is equivalent to deleting data for the purposes of Article 17 of the GDPR. In this regard, the French data protection Authority suggested that, to comply with the obligation pursuant to art. 17 in the blockchain context, it is not necessary to erase the data but, rather, alternative means could also do. The concrete example that the French guarantor suggests is the following: since blockchains are made up of encrypted data that can only be reached through a key, the private key needed to access the ledgers could be destroyed, thus performing out an operation that is in fact equivalent to the erasure of the data.[35] This is the mechanism that is used today by several biobanks, as will be seen later in the discussion, precisely to be compliant with the *right to be forgotten*.

4. *The twofold difficulty when dealing with data controllership in Blockchain environments: identification and obligations*

Another very interesting yet controversial area of privacy law to look at through the lens of blockchain technology is that of the data controller, and in particular its identification. Blockchains are polycentric networks where we have many actors influencing the processing of data. Art. 4 par. 7 GDPR informs us that the data controller is the natural or legal person, public authority, agency, or other body which, alone or together with others, determines the purposes and means of the processing of personal data. GDPR also contains the notion of joint controller: art. 26, par. 1 of the Regulation

grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
(4) the personal data have been unlawfully processed;
(5) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
(6) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

General Data Protection Regulation (GDPR), Article 17: *Right to erasure ("right to be forgotten")*.

[32] On the right to be forgotten, see S. Scagliarini, *Digital identity and privacy protection*, presented at Pisa Group Association's Annual Conference, Genoa, 18-19 June 2021 "Constitutional law and the challenges of technological innovation" , 9 *et seq.*: article 17 of the GDPR has been criticized as it reduces the discipline of the right to be forgotten to the mere "cancellation" of data; but, as clarified by the Italian Supreme Court in the decision no. 19681/19, "when dealing with the right to be forgotten we are actually referring to at least three different situations: that of those who wish not to see a second publication of news (that were legitimately spread in the past) relating to events, when a certain time has passed between the first and second publication; that, connected to the use of the internet and the availability of news online, consisting in the need to place the publication, which legitimately took place many years earlier, in the current context [...]; and that, finally, dealt with in the Google Spain ruling of the European Court of Justice, in which the data subject asserts the right to have data deleted".

[33] European Court of Judgment, Judgment of the Court (Grand Chamber) of 13 May 2014. *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*.

[34] Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR), Right to erasure*.

[35] National Commission on Informatics and Liberty (Commission Nationale de l'Informatique et des Libertés - CNIL), *Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data*, November 6, 2018.

states that it is possible to have two or more controllers in a data-processing situation. This occurs when two or more controllers jointly determine the purposes and means of the processing.

This is indeed a very hot area of privacy law right now, to the extent that there have been several recent judgments where the European Court of Justice has interpreted the notion of joint controllership in interesting ways. For example, in the *Wirtschaftsakademie schleswig holstein* case,[36] the court essentially indicated that when a person accepts the means and purposes of data processing that have been specified by someone else, and then benefits from this agreement in some way, it can be assumed that that person also actively determines the means and purposes of data processing and consequently becomes a data controller. This orientation was confirmed, only a few weeks later, in a case relating to Jehovah's Witnesses[37] in which the Court reaffirmed this reasoning based on this interpretation of the notion of joint controllership: the Court also added that, to be a data controller, it is not necessary to have physical access to the personal data in question. Again, the court indicated that a natural or legal person who exercises an influence on the processing or on personal data for their own purposes can be considered a data controller. So, recent case law on joint controllership embraces a very broad view of the concept; it can then be affirmed that anyone who consents to someone else's data processing and then takes advantage of it for their own purposes becomes the data controller.

The question arising is what this broad definition of both controllership and joint controllership could mean in the blockchain context. In this regard, the French Authority (CNIL) released a document in 2018 in which they stated that participants, who have the right to "write" on the chain and who decide to send data for validation by the miners (which will be discussed shortly), can be considered as data controllers.[38]

4.1. *Actors of blockchain*

There are several actors that participate in blockchain networks and that could, as a matter of principle, be in possession of the requirements to be qualified as data controllers. Can, for instance, core developers be considered as data controllers? Core developers are the people who create the software, the real IT structure on which a particular blockchain network is based. It may seem that core developers cannot be really considered data controllers since, while retaining a decisive influence on the means insofar as they determine the appearance of the software (therefore they certainly have a say), the objective of their role is usually that of assigning powers and responsibilities to other stakeholders such as, for example, directors, through IT programming. Furthermore, the actual personal data does not pass through the IT systems of the core developers. In short, they limit themselves to supplying the technology.[39] However, this does not necessarily exclude that they may be joint controllers. In the case of *Jehovah's Witnesses*, for example, the European Court of Justice has decided that it is not necessary for all joint controllers to have access to personal

[36] European Court of Justice, Judgment of the Court (Grand Chamber) of June 5, 2018: *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH* in relation to whether an administrator of a fan page on a social network qualifies as a joint controller with regards to the processing of personal data of visitors to the page and the competence of a supervisory authority. The CJEU held that an administrator of a fan page hosted on a social network must be regarded as a controller under Article 2(d) of the Data Protection Directive 95/46/EC.

[37] European Court of Justice, Judgment of the Court (Grand Chamber) of 10 July 2018, *Tietosuojavaltuutettu and Jehovan todistajat - uskonnollinen yhdyskunta,* where the Court has held that religious groups undertaking door-to-door preaching activities in specific geographical areas were subject to the Data Protection Directive (95/46/EC).

[38] According to the French Authority, indeed, blockchain participants define the purposes (objectives pursued by the processing) and the means (data format, use of blockchain technology, etc.) of the processing. More specifically, the CNIL considers that "the participant is a data controller: when the said participant is a natural person and that the personal data processing operation is related to a professional or commercial activity (i.e., when the activity is not strictly personal); when the said participant is a legal person and that it registers personal data in a blockchain". National Commission on Informatics and Liberty (Commission nationale de l'informatique et des libertés - CNIL), *Solutions for a responsible use of the blockchain in the context of personal data*, September 2018, available at www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf

[39] M. Schellekens, *Conceptualizations of the controller in permissionless blockchains*, in *Journal of Intellectual Property, Information Technology and E-Commerce Law*, vol. 11, 2020, especially par. 47.

data.[40]

Then we have the so-called *miners*. The miners are those who accumulate cryptocurrency on their computers, the so-called *farms*, which are computers entirely dedicated and adapted for this purpose. They have, in the same way as developers, a decisive influence on the means also because of their active role in the governance of the blockchain but, still in almost all cases they do not have an influence on the purposes of data processing.[41]

Then there are the *nodes*, which are the many computers in which the blockchain is stored. There is relatively broad agreement that nodes could qualify as data controllers[42] insofar the nodes determine their purpose for participating in the network and to the extent that they have access to all data stored in the ledgers. However, the possibility of defining nodes as controllers is disputed.[43]

What emerges is that to identify the data controller in a blockchain environment is a laborious task. To fulfill this task, it is necessary to investigate the precise characteristics of the blockchain used in the specific case of use; the data controller (or controllers) must be identified on a case-by-case basis.

[40] European Court of Justice, Judgment of the Court (Grand Chamber) of 10 July 2018, *Tietosuojavaltuutettu and Jehovan todistajat - uskonnollinen yhdyskunta.*

[41] This view is confirmed by the French data Authority (CNIL) in its 2018 document precisely in the sense that "miners are only validating transactions submitted by participants and are not involved in the object of these transactions: therefore, they do not define the purposes and the means of the processing", National Commission on Informatics and Liberty (Commission nationale de l'informatique et des libertés - CNIL), *Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data*, 6 November 2018; See also M. Schellekens, *Conceptualizations of the controller in permissionless blockchains*, par. 17.

[42] On this topic, M. Florian, S. Henningsen and S. Beaucamp, *Erasing Data from Blockchain Nodes*, presented at 2019 IEEE European Symposium on Security and Privacy Workshops, IEEE (Institute for Electrical and Electronics Engineers), 17-19 June 2019, 367-376; see also J. Czarnecki, *Who is the data controller in a blockchain?*, in *Newtech Law Blog*, August 20, 2018; and C. Andronicou, *Blockchain and the GDPR: Clash of the Titans*, in *International Network of Privacy Law Professionals*, August 2021.

[43] In this connection, P.J. Pesch and C. Sillaber, *Distributed ledger, joint control? - Blockchains and the GDPR's transparency requirements*, in *Computer Law Review International*, vol. 17, 2017, 166 ff.; See also M. Berberich and M. Steiner, *Blockchain technology and the GDPR how to reconcile privacy and distributed ledgers*, in *Eur. Data Prot. L. Rev.*, 2016, vol. 2, 422 and seq.

4.2. *Obligations*

After investigating who can be considered the data controller, the second question is: what does it mean, for a subject, to actually be the data controller in a blockchain environment? The first thing to point out is that, none of the actors we have examined have full control of what happens to the personal data present on the blockchain network. So, for example, if one were to accept that the node is the data controller in relation to the personal data stored on the blockchain, the node will not be able to realize the right of access pursuant to art. 15 GDPR, since all nodes will be encrypted with the hash function and this could constitute a major obstacle to comply with GDPR's obligation of correctly supplying information to the data subject about his or her data; in the same way, then, the nodes will never be able to operate independently pursuant to the right to be forgotten *per* art. 17.

A very interesting element that highlights the factual inability of these actors to comply with the obligations imposed by the GDPR, and which motivates the tension between the GDPR and blockchain, can be found under art. 26 GDPR: its first paragraph states that, where there are joint controllers who determine in concert the purposes and means of the processing, they must conclude an agreement that establishes their respective responsibilities. Therefore, the third paragraph of article 26 adds that "regardless of the provisions of the agreement referred to in paragraph 1, the data subject may exercise his rights pursuant to this regulation towards and against each data controller".

So, if we consider that in blockchains (in particular the public and permissionless types) there are many different actors and several of these can actually qualify as data controllers, a question spontaneously arises: who of those many parties should actually address the data subject and what happens if the latter decides to contact one of the joint data controllers who is in fact unable to fulfill the obligation imposed on him under the GDPR? Even this, in the absence of an *ad hoc* discipline, will be assessed on a case-by-case basis. It is certain that in private and permissioned blockchains (but also in consortium-type blockchains) the solution could be less strenuous, since networks of this type are characterized by well-defined governance structures, capable to establish the roles of the different actors and

the interactions between them; more difficult, on the other hand, is to navigate within the framework of public and permissionless blockchains.

5. *"Block" biobanking perspectives and advantages for healthcare*

We have analyzed the relationship between the GDPR and blockchains focusing exclusively on its tensions and contrasting elements. Before concluding, however, it is also appropriate to focus on the positive aspects of the relationship between Europe's main law source on privacy and the revolutionary blocking technology. Of course, the current debate focuses more massively on the discord that exists between them, but people are also starting to realize that blockchain is really a tool that could bring a variety of benefits and that it is totally capable of contributing to the development and enrichment of the very culture of privacy regulation. Let's see how this is possible by using the healthcare domain as a key to understanding.

Blockchain is a class of technologies that can be exploited in several ways. However, we have noticed how it is not to be understood as a technology that is automatically useful for the protection of personal data nor automatically advantageous for the goals of the GDPR. However, it is a very malleable technology and, when molded in the right shape, it can help accomplish some of these goals (e.g., to adapt to the GDPR, it appears crucial to opt for a private and permissioned blockchain model or, at least, a public-permissioned consortium).

Some uses of blockchain can be beneficial with regard to the aspects of accountability and transparency. Having a ledger that is distributed among many different actors, equipped with a timestamp and whose operation is based on extremely rigid parameters of automaticity and certainty, could be the ideal tool to keep track of the obligations that the data controllers must put in place to comply with the GDPR in the phases of the data processing impact assessment (DPIA), so that they can demonstrate that they have acted in accordance with their obligations, complete with certain date; it could function as a guarantee system through which data subjects can monitor who has had access to their data and at what time, and with which they can quickly and accurately obtain all the information they are entitled to pursuant to art. 15 GDPR, with grand benefits from a transparency point of view; or again, it could be greatly helpful for the collection of consent to the processing of data.

5.1. *Examples of blockchain-based biobanks in practice*

In this regard, there are several examples of biobanks that have been conceived precisely in this spirit, namely the search for a use (and, even before, a modeling) of blockchain as adherent as possible to both the dictates of the GDPR and the special needs of medical research. A research group from the University of Malta has devised, in the context of biobanks, a solution based precisely on the aspects of gathering consent and that even aims to solve the apparently diabolical problem of blockchain's compliance with the right to be forgotten, and published their solution in Nature.[44] The researchers talked about dynamic consent. Dynamic consent aims to give people the opportunity to be better informed about their consent choices and, in general, about the ongoing research process, and to maintain guarantees and control over how their biological samples and data are used. This consent system would also allow research participants to access a record of their consent decisions. Participants can review previous decisions and change their decision. In other words, even if the participant signed a consent form at the beginning of the process, that would not be the last word on his or her consent status. They can, in fact, update or withdraw their consent at any time. Therefore, this peculiar biobank, called Dwarna, allows research partners to learn more and get involved in genomic research. Search Partners log into the Dwarna Portal using their alias and password to learn about ongoing searches. If they are inclined to participate in any study, they can indicate it by flipping a switch for consent. They can also withdraw this consent at any time using an identical mechanism or request the deletion of their data and the destruction of their bio-sample from the biobank. But the examples of blockchain-based biobanks are

[44] For Dwarna's white paper, see N. Mamo, G.M. Martin and M. Desira, *Dwarna: a blockchain solution for dynamic consent in biobanking*, in *European Journal of Human Genetics*, vol. 28, 2020, 609-626.

several:[45] MedRec[46] is also (mainly) a blockchain solution that stores sensitive personal information in a more traditional and centralized off-chain database from which data can be removed. The blockchain itself only stores the hashes of this data and preserves a ledger containing patient permissions to doctors to access the data.

5.2. *Other beneficial uses of blockchain for patient care*

And indeed, blockchain technology can be of great help for access control, management of medical records and their sharing, but also for verifying the correctness of the financial statements and procedures of a healthcare company. Undoubted benefits have also been found in the pharmaceutical field, where it is necessary to manage drug prescriptions with great precision and it is essential to better organize drug supply chains, according to parameters of certainty and efficiency.[47] Furthermore, in the field of healthcare, the aspect of the patient's control over his health data and the relationship between patient and doctor is of central importance, and indeed, blockchain opens new horizons also with regard to Remote Patient Monitoring (RPM), namely the set of advanced systems that allow doctors to obtain real-time information on their patients remotely with the help of the wireless-communication system, with the effect of reducing time and costs for the patient, and also providing medical assistance of quality to the patient.[48]

In the digital age, preserving patient data privacy is crucial. The data present in the collections of healthcare facilities, as we have seen, are very sensitive and very expensive. Therefore, they represent a primary target for cyber-attacks. Blockchain technology is indeed very robust against attacks and failures and provides several access control methods.

5.3. *Blockchain in health data protection: conclusions*

Blockchain seems to have all the credentials to protect data and improve the quality of patient care. Its cornerstones, based on shared immutable data organized in a network of nodes where transactions are stored in a digital ledger, have already been applied in many sectors such as banking and finance to protect data from intruders. There are various applications in the health field, such as for Electronic Health Record (EHR), for genomics, biomedical, pharmaceutical science, and laboratories in which the blockchain is integrated with existing applications or provides the tools to create new ones. Therefore, it seems that blockchain, used in a virtuous and targeted way, paints a picture full of positivity regarding health data and healthcare as a whole.

Examples like these really highlight how the arguments supporting the total discord between blockchains and the GDPR and the absolute uselessness or even dangerousness of this class of technologies with respect to privacy regulation really lack vision and indeed constitute an obstacle to one of the very guiding principles of the GDPR itself, which is to support the development of technology, through principles and tools that can adapt to the rapid and, often, even subversive changes of society typical of this era of the digital economy. However, the study highlighted that blockchain is a multiform, malleable, and changing class of technologies, with technical characteristics and governance arrangements that can be very different from each other. For this reason, the compatibility of these tools with the Regulation can only be assessed on a case-by-case basis: just as it can be modeled in a beneficial and risk-free form, blockchain can also take on shapes that put a strain on the principles of privacy regulation, which are highly worthy of being taken into consideration as a reflection of common sense, as well as of commendable interest and effort by European legislators towards the

[45] In fact, just three years after what is conventionally identified as the birth date of the blockchain (Satoshi Nakamoto's 2008 white paper), Estonia had already partnered with the private sector to begin archiving medical records in blockchains. Since then, more use cases of blockchains in the healthcare sector have emerged in the literature. See M. Mettler, *Blockchain Technology in Healthcare: The Revolution Starts Here*, presented at 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services, September 2019, 2.

[46] For MedRec's white paper, see A. Ekblaw, A. Azaria, J.D. Halamka and A. Lippman, *A case study for block-chain in healthcare:"MedRec" prototype for electronic health records and medical research data*, presented at *IEEE Open & Big Data Conference*, 22-24 August 2016.

[47] On this topic, A.D. Shetty, S. Shenoy and D. Sreedhar, *Traceability of counterfeit drugs in pharma supply chain through Blockchain Technology - A Systematic Review of the Evidence*, in *Research Journal of Pharmacy and Technology*, vol. 15, February 2022.

[48] J. Hathaliya, P. Sharma and S. Tanwar, *Blockchain-based Remote Patient Monitoring in Healthcare 4.0*, 87.

noble dreamscape of data protection.

6. *Concluding thoughts: should blockchain be considered an enemy or an ally of the GDPR?*

What emerges when analyzing blockchains from a GDPR perspective is an undoubted climate of tension. This tension can essentially be linked to two main antinomies: the antinomy between the centralization, on which the regulatory pattern of the GDPR is built (identification of a data controller, i.e., a center of imputation of obligations to be performed towards the data subject, according to the privacy-by-design and by-default[49] principles) and decentralization, major bulwark of the blockchains, which generates considerable problems regarding the configuration of responsibility under current privacy law; the antinomy between the mutability, required for the purposes of GDPR's *right to be forgotten*, and the immutability of blockchain ledgers, contained in realistically-indecipherable algorithms. These arguments have not escaped the attention of regulators and a whole range of experts in this sector. These factors have triggered a debate about whether the GDPR stands in the way of an innovative EU-based blockchain ecosystem. Some have expressed their support for a revision of the GDPR, and claim that blockchains should benefit from an altogether exemption of the EU data-protection framework. According to those, in fact, the very existence of the GDPR would stifle the free development and potential of blockchain in Europe, and this could leave Europe behind other jurisdictions on the planet which, not having the "burden" of the GDPR, will be able to exploit all the advantages of the novelties that this technology has in store for humans.[50] Others stressed the primacy of regulation and said that if blockchain can't comply with the GDPR, that means it is likely to be an innovation that should be abandoned as it is unable to achieve established public-policy goals.[51]

So, do we really need to change or even abolish the GDPR in an attempt to make Europe a competitive environment for data-driven economies, or should we leave blockchain technology stranded, given its apparent inability to comply with the law? Neither of these is the case or, rather, the solution lies somewhere in the middle. The GDPR is a principle-based regulation and has a whole range of regulatory mechanisms that were designed precisely to encourage the emergence of new technologies, such as certification mechanisms.[52] Furthermore, many of the existing tensions are basically reduced to simple lack of sufficient specification in the text of the law, or interpretation gaps. If we had more indications from the regulatory authorities, for example, on how the term "erasure" is to be interpreted in accordance with the specificities of DLT structures, together with a contribution from the people who develop and prepare blockchain networks aimed at setting up more "friendly" governance mechanisms (in the sense of taking into account the inevitable arrival of a regulatory eye that will, quite understandably, be looking for guarantees on the processing of personal data) it may well be possible to overcome those tensions that today represent a wall.

On the other hand, however, while there are certainly many tensions between different key features of blockchains and some cornerstones of European data-protection legislation, many of the related uncertainties should not be traced back only to the specific characteristics of this technology. Rather, by moving the magnifying glass to the GDPR, it can be highlighted that parts of it are to be

[49] The principles of privacy-by-design and privacy-by-default are dealt with in art. 25, paragraphs 1 and 2, GDPR. Recitals 24-29 define the techniques and measures to be implemented to ensure their compliance. In this regard, M. Midiri and S. Piva, *L'interesse pubblico come base giuridica e come finalità del trattamento dei dati personali*, in *Il "nuovo" codice in materia di protezione dei dati personali*, S. Scagliarini (ed.), 33.

[50] European Parliament - Panel for the Future of Science and Technology in the context of European Parliamentary Research Service (EPRS), *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?*, July 2019, especially 1.

[51] D. Meyer, *Blockchain technology is on a collision course with EU privacy law*, in *The Privacy Advisor*, 27 February 2018, blog article available at https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/.

[52] Through the certification mechanism, data controllers obtain and benefit from the certification of an independent third party in order to demonstrate the compliance of their data-processing operations. Garante per la protezione dei dati personali (Italian data protection Authority), *FAQ in materia di certificazione e accreditamento ai sensi del GDPR*, available at www.garanteprivacy.it/regolamentoue/certificazione-e-accreditamento.

analyzed outside the specific context of blockchains. Some aspects of the GDPR (as underlined by the European Parliament itself in 2019[53]), such as data controllership and joint controllership, or the *right to be forgotten*, would require more regulatory effort (also from the Member States' legislators) in the sense of clearer rules that consider the specificities of use cases in a widespread manner. Similarly, we have seen how decisive the interpretative contribution of the Courts and the major independent European Authorities is. Greater coordination between the Authorities in clarifying the interpretation of the rules and key concepts of the GDPR would be auspicious.

[53] European Parliament - Panel for the Future of Science and Technology in the context of European Parliamentary Research Service (EPRS), *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?*, July 2019, 101.