Borroni A, Zambardino F, 'Distributed Ledger Technologies (DLTs) and right to health: the impact of blockchain in the healthcare sector' (2023) 2 EJPLT, 93 - 110.
DOI: https://doi.org/10.57230/EJPLT232ABFZ

EJPLT
ISSN 2704-8012



Distributed Ledger Technologies (DLTs) and right to health: the impact of blockchain in the healthcare sector

Distributed Ledger Technologies (DLTs) e diritto alla salute: l'impatto della blockchain nel settore sanitario

ANDREA BORRONI
Associate Professor of Comparative Law
University of Campania Luigi Vanvitelli

FABIO ZAMBARDINO
Post-doctoral fellow
University of Campania Luigi Vanvitelli

Abstract

The aim of this contribution is to understand whether and how the blockchain technology can be used in the health sector, analyzing the ways in which its incorporation into the management of health data infrastructure might have the potential to create a more efficient national healthcare system.

L'obiettivo del presente contributo è quello di analizzare se e come la tecnologia blockchain possa essere utilizzata nel settore sanitario, verificando le modalità in cui la sua incorporazione nella gestione dell'infrastruttura dei dati sanitari potrebbe avere il potenziale per creare un sistema sanitario nazionale più efficiente.

© The author(s) 2023, published by Suor Orsola Benincasa Università Editrice. This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Blockchain; Healthcare; Electronic Health Record; Data protection; Telemedicine.

Summary: Introduction – 1. The main features of blockchain technology. – 2. How blockchain fits into the healthcare sector. – 3. Different types of blockchain. – 4. Health protection and data protection. – 5. Blockchain and telemedicine. – Conclusive remarks.

Introduction.

The use of new technologies in the healthcare sector has only recently started to develop, more for medical-diagnostic use than for the purpose of facilitating healthcare organisation *stricto sensu*.[1]

The prompt advent of the Internet of things (IoT) paradigm has introduced several innovative elements, generating major improvements in terms of, *inter alia*, electronic medical records, data sharing on the production and circulation of drugs, in relation to insurance information, and in terms of facilitating remote assistance.[2]

From a strictly legal point of view, the ability of the existing rules to reshape themselves to intercept the reorganisation of the law caused by the

* Even though the article is the product of common critical analysis and considerations, Andrea Borroni authored paragraphs: 3, 6, 7 and Fabio Zambardino authored paragraphs: 1, 2, 4, 5.

[1] The introduction of digitisation in the health sector has its origins in the reform of the public administration, conceived since the times of the 1999 Bassanini reforms, but at that stage it was soon abandoned due to the difficulty of the public administration in accepting such significant transformations, to the absence of a suitable network and digitisation of the administration, and, in any case, to the backwardness of the state and regional administrative context incapable of accepting such innovations. For a reconstruction of digitalization in public administration see G Duni, *L'Amministrazione digitale* (Giuffrè 2008); F Bassanini, 'Twenty years of administrative reformsin Italy' (2009) 3 Review of Economic Conditions in Italy, 369 ff; E Carloni, 'L'amministrazione aperta. Regole e limiti dell'open Government' (2014) Orizzonti di Diritto Commerciale; F Martines, 'La digitalizzazione della pubblica amministrazione' (2018) 2 Medialaws; R Cavallo Perin, D U Galetta (ed.), *Il diritto dell'Amministrazione Pubblica digitale* (Giappichelli 2020). In 2005, with the approval of the Digital Administration Code, a start was then made on giving shape to this project, in particular in the light of articles 43 and 44 where it is stipulated that any document, which by law or regulation must be stored, may be reproduced and stored on computer support, if the relevant procedures are carried out in such a way as to guarantee conformity with the original documents and comply with the Guidelines, but then leaving the possibility of maintaining storage in paper form. E Catelani, 'Nuove tecnologie e tutela del diritto della salute: potenzialità e limiti dell'uso della Blockchain' (2022) 4 Federalismi, 214. It was only in 2012 that these objectives were transformed into concrete regulations, and in particular with Article 47-bis of Decree-Law No. 5/2012, converted, with amendments, by Law No. 3 of 4 April 2012), which speaks of digital healthcare and with the approval of Decree-Law No. 179 (later converted, with amendments, by Law No. 221 of 17 December 2012), which more explicitly dematerialises medical records, which no longer need to be made into a paper document and signed by healthcare personnel, even if they were already drawn up by the health authorities. 221 of 17 December 2012), which more explicitly dematerialised the medical record, which in fact no longer needs to be turned into a paper document and signed by the healthcare personnel, even if it is already in the so-called computerised medical record, but is limited to being in electronic format in all respects. *Ibid.*

[2] See for a general overview M Durante, U Pagallo (eds.), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, (Giappichelli 2013).

involvement of innovative technologies is an indispensable condition for the full affirmation of rights in the encounter between health and technological innovation and thus, in the final analysis, for the concrete implementation of the constitutional guarantee of health as a fundamental right of the individual and interest of the community.[3]

In particular, an important role can be played by the blockchain that, due to its operational versatility, makes it possible to shape a distributed database for the management of common transactions, in which traceability and unchangeability are guaranteed; furthermore, the executive continuity of the system is ensured by the union of widespread control (peer to peer), with cryptographic techniques.[4]

Given the premises, this paper aims to provide, firstly, a brief examination of the functioning of the distributed ledger system and, secondly, to investigate the actual possibility of finding a point of balance between the need to protect the privacy of the subject concerned and that of health protection, in order to favour a concrete evaluation of the suitability of personal data protection to act as an extreme boundary to the right to health.[5]

1. The main features of blockchain technology.

In terms of definition, the blockchain can be considered a public ledger containing the history of all transactions and/or operations entered into it.

Its structure consists of a concatenated list of data, into which the nodes of the network – *i.e.,* computers connected to the ledger – enter blocks of information according to the rules of the implementation system.[6]

A chronological digital ledger, therefore, whose contents can be verified by any device with an internet connection. Each blockchain is then encrypted and

[3] F Aperio Bella, 'L'accesso alle tecnologie innovative nel settore salute tra universalità e limiti organizzativi (con una postilla sull'emergenza sanitaria)' (2020) 1, PERS. AMM., 220. See also G Pascuzzi, U Izzo, 'Le problematiche giuridiche connesse all'utilizzo delle nuove tecnologie in sanità' (2012), psychiatryonline.it, 155-163.

[4] M Farina, 'Blockchain e tutela della salute: verso la riorganizzazione dei sistemi sanitari?' (2020) 21, Federalismi, 173.

[5] Two principles, those enunciated above, which are certainly not opposed, but rather complementary, and which constitute the expression, with different nuances, of the common value of human dignity and personality referred to in Article 2 of the Constitution. On the "open" nature of the enumeration contained in Article 2 of the Constitution, see A Barbera, 'Commento all'art. 2 della Costituzione', in G Branca (ed.), *Commentario della Costituzione italiana* (1995) Zanichelli; P Rescigno, 'Personalità (diritti della)', *Enciclopedia Giuridica* XXIII (1990) 1 ff; V Zeno Zencovich, 'Personalità (diritti della)', *Digesto delle Discipline Privatistiche* XIII (1995) 453 ff. See also E Frosini, 'Tecnologie e libertà costituzionali, in G Comandé, G Ponzalli (eds.), *Scienza e diritto nel prisma del diritto comparato* (Giappichelli 2004), 189, who, still on the subject of the relationship between technology and privacy, states how new technological discoveries have represented and continue to represent a development of freedoms; indeed, freedoms have been able to greatly increase and expand towards new frontiers of human action precisely because of technological progress.

[6] A Wright, P De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia (Panthéon-Assas 2015) 6.

organised into groups of smaller transactions called blocks.[7]

The content of this database is verified through a mechanism that requires the authorisation of all participants in the blockchain since, once information has been entered into the system, it cannot be deleted unless 'changes are approved by the majority of the computing power of the entire blockchain'.[8]

Moreover, a copy of the blockchain is stored on all the computers in the network that are periodically synchronised to ensure that all users have the same shared database.[9]

The essential element of such a system is decentralisation, which describes the process of diversification and dispersal of power from a central authority,[10] the basis of which is to be found in the creation of a *sui generis* network through which transactions can be carried out in a more secure and flexible manner.[11]

This, in fact, allows the blockchain greater resistance to attacks since, if one or more nodes stop functioning, however, "trust" can be maintained by relying on the other nodes.

Unlike centralised systems, where the administrator acts as the pivot point for each user instance and where storage is carried out at a single level, with a consequent risk of data loss,[12] in distributed structures, each node acts as a depository of a copy of the registry and all changes that are made are subject to the approval of the entire community of nodes, based on (computer) consensus rules established in the algorithm.[13]

Finally, a further strong point is outlined by the guarantee of information transparency since users have a fully verifiable register at their disposal.[14]

2. How blockchain fits into the healthcare sector.

The use of Distributed Ledger Technologies, such as blockchain, has extended from the cryptocurrency market to other fields, including, for instance, the privacy sector.[15]

---

[7] A Borroni, 'Blockchain: Uses and Potential Value', in A Borroni, *Legal Perspective on Blockchain Theory, Outcomes, and Outlooks*, (ESI 2019) 5.

[8] *Ibid.*

[9] Wright, De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (n 6) 6-8.

[10] R Böhme and others, 'Bitcoin: Economics, Technology, and Governance' (2014) 29 J. ECON. PERSP., 219-220.

[11] M Abramowicz, 'Cryptocurrency-Based Law', in *GWU Law School Public Law Research Paper* (2015) 6-7.

[12] M Giuliano, 'La blockchain e gli smart contracts nell'innovazione del diritto nel terzo millennio' (2019) DIR. INFORM., 996.

[13] Borroni, 'Blockchain: Uses and Potential Value' (n 7) 6-7.

[14] Abramowicz, 'Cryptocurrency-Based Law' (n 11) 9. A level of transparency that, according to the author, should ensure a higher level of adoption of blockchain technology. See, on the topic of transparency, Iorio, *A Modern Approach to Global Tax Transparency and Beneficial Ownership Registers: Forget Sunlight, Is Blockchain the Best Disinfectant?* (New York Law School 2020); PK Medhi, *Role of Blockchain Enabled Transparency in Risk Management and Sustainability of the Complex Global Supply Chains*, (Bennett University 2019).

[15] For an analysis of the different use cases of the blockchain technology, be permitted a reference to Borroni, 'Blockchain: Uses and Potential Value' (n 7) 7.

In particular, the need for decentralisation lies in the growing concern of users about the loss of control over their personal data stored on the Internet.[16]

In this respect, the very structure of blockchain technology would allow data privacy to be preserved; however, such architectures can sometimes prove vulnerable to metadata analysis. Consequently, if not properly designed, 'decentralized infrastructures intended to promote individual privacy and autonomy might turn out to be much more vulnerable to governmental or corporate surveillance than their centralized counterparts'.[17]

Given the technological substratum discussed in the previous section, the reason for the interest of researchers from a wide range of fields in the potential of DLTs in terms of data management is inherent in the advantages that this could bring in the health sector.

In that field, in fact, distributed registers promise a wide range of applications and functions. Specifically, 'blockchain helps healthcare researchers uncover genetic code by facilitating the secure transfer of patient medical records, managing the drug supply chain, and facilitating the safe transfer of patient medical records'.[18]

Prima facie, a verifiable solution concerns the difficulty of healthcare institutions in sharing information, communicating data, examinations and opinions on the same case or person, providing effective tracking of patient information, and hopefully reducing cases of clinic liability.[19]

The benefit lies in the fact that the various "nodes" could enter all the health information of the individual patient in a system of "blocks" and that, once entered, they could no longer be modified and would only be readable with the required authorisations.[20]

---

[16] Some scholars, in this regard, refer to the emergence of a true virtual identity; personal identity, in the current context, also leads to a new dimension, namely that of information technology, in which personal identity is necessary for the execution of a series of actions, mostly of a patrimonial nature – e.g. the use of credit cards on the web, the various commercial transactions, and even social networks. On this point, S Rodotà, 'Quattro paradigmi per l'identità', in *Vivere la democrazia* (Laterza 2018) 20 ff; G Alpa, 'L'identità digitale e la tutela della persona. Spunti di riflessione' (2017) CONTR. IMPR., 725; G Resta, 'Identità personale e identità digitale' (2007) DIR. INFOR.

[17] P. De Filippi, 'The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies (2016) 7 J. PEER. PROD., 1. The author emphasises that despite the obvious advantages they offer in terms of data sovereignty, decentralised architectures also have features that, if not taken into due consideration, could ultimately compromise users' privacy. Indeed, '[w]hile they are capable of preserving the confidentiality of data, decentralized architectures cannot easily protect themselves against the analysis of metadata'. *Ibid.*

[18] A Haleem and others, 'Blockchain technology applications in healthcare: An overview' (2021) INT'L J. INTELLIGENT NET., 132-133.

[19] MS Gross, RC Miller Jr., 'Ethical Implementation of the Learning Healthcare System with Blockchain Technology', in *Blockchain in Healthcare Today* (Berman 2019). For a general overview of liability in healthcare see P Stanzione, V Zambrano, *Attività sanitaria e responsabilità civile* (Giuffrè 1998); M Bassini and others, 'Sistemi di intelligenza artificiale, responsabilità e accountability. Verso nuovi paradigmi?', in F Pizzetti (ed.), *Intelligenza artificiale, protezione dei dati personali e regolazione*, (Giappichelli 2018) 333 ff.

[20] Catelani, 'Nuove tecnologie e tutela del diritto della salute: potenzialità e limiti dell'uso della Blockchain' (n 1) 219. This represents a purpose from which treating physicians and healthcare facilities can equally benefit to reduce their possible liability, especially where recognised healthcare guidelines have been

It is possible to state how the healthcare system is required to 'to do more with less, find new ways to treat patients more efficiently, and deliver care in alternate settings that help keep patients out of the hospital'.[21]

It would be desirable, in this regard, to improve collaboration between providers through well-organised data sharing systems, to increase the capacity of healthcare facilities and, at the same time, of operators to circulate information, making it more accessible to the majority of those involved with consequent advantages in terms of speed and, above all, economics.[22]

Compared to traditional healthcare systems, in fact, the application of blockchain in this sector has the connotations of preventability, immediacy and interconnection of information.[23]

---

followed, as provided for by Law No. 24/2017 (the so-called Gelli-White Law). The Gelli-Bianco law, adopting the so-called "double track" system, recomposed the interpretation of Article 1228, bringing healthcare workers back into the group of the debtor's auxiliaries who, unlike the latter, who are contractually and objectively liable for their wilful and negligent acts, are liable for their non-contractual and negligent acts. The liability of the healthcare facility that, in the performance of its obligation, makes use of the work of third parties, on the other hand, has been explicitly qualified as "contractual" by the recent reform law, which precisely recalls Articles 1218 and 1228 of the Italian Civil Code (Art. 7, paragraph 1 of the Law). See A Procida Mirabelli di Lauro, 'Inadempimento e causalità "materiale": perseverare diabolicum' (2020) 1 DANNO & RESP., 76. On liability of structures, see amplius G D'Amico, 'Il rischio della "causa ignota" nella responsabilità contrattuale in materia sanitaria' (2018) DANNO RESP., 357 ff; R Pardolesi, R Simone, 'Tra discese ardite e risalite: causalità e consenso in campo medico' (2018) 1 FORO IT., 3582 ff; R Pardolesi, R Simone, 'Nesso di causa e responsabilità della struttura sanitaria: indietro tutta!' (2018) 1 DANNO RESP., 10 ff; A Procida Mirabelli di Lauro, M Feola, 'La cooperazione mancata: sopravvenuta impossibilità della prestazione e imputabilità dell'inadempimento' (2019) COMPARAZIONE DIR. CIV., 33 ff; Stanzione, Zambrano, *Attività sanitaria e responsabilità civile* (n 19); Toscano, 'Il difetto di organizzazione: una nuova ipotesi di responsabilità? (note to Court of Monza June 7 1995)' (1996) RESP. CIV. PREV., 389 ff; I Rapisarda, 'La privacy sanitaria alla prova del mobile ecosystem. Il caso delle app mediche' (2023) 1 LEGGI CIV. COMM.,184; C Irti, 'L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano' (2023) 1 PERS. MERC., 32-49; M Magliulo, R Pardolesi, 'Pluralità di nessi di causa e paziente allo sbaraglio' (2019) DANNO RESP., 256 ff; F Piraino, 'Il nesso di causalità materiale nella responsabilità contrattuale e la ripartizione dell'onere della prova' (2019) GIUR. IT., 709 ff; G Comandé, 'La riforma della responsabilità sanitaria al bivio tra conferma, sovversione, confusione e ... no-blame giurisprudenziale' (2016) RIV. IT. MED. LEG. the author emphasises how while the natural reference to "liability of the doctor" implicitly referred to an individual contractual liability for inexact fulfilment of the obligations contractually assumed by the professional, subsequently the attention of jurisprudence began to shift towards the extra-contractual liability of the professional whose relationship with the patient appeared difficult to qualify in strictly contractual terms. By the same author, G Comandé, 'Dalla responsabilità sanitaria al no-blame regionale tra conciliazione e risarcimento' (2010) DANNO & RESP., 977-988; G Comandé, 'Le «regioni» della responsabilità sanitaria e il governo del risarcimento', in *"Liber Amicorum" per Francesco D. Busnelli. Il diritto civile tra principi e regole* (Giuffrè 2008) 529-544. See also, FD Busnelli, 'Il fattore "potenziamento": salute, medicina e deontologia al vaglio delle nuove tecnologie' (2017) RESP. MED., 315 ff; A Borroni, 'Gli obblighi a carico del personale e dei liberi professionisti che operano nella struttura, in F Gelli and others, *La nuova responsabilità sanitaria e la sua assicurazione dopo la legge Gelli-Bianco* (Giuffrè 2017) 67-74.

[21] Borroni, 'Blockchain: Uses and Potential Value' (n 7) 41.

[22] A Deborah and others, 'Blockchain: A Possible Alternative to Achieving Health Information Exchange (HIE)' (2020) 8 INT. J. INNOV. RES. SCI. ENG. TECHNOL., 159-160.

[23] Through the network, using portable mobile devices, medical personnel can constantly perceive, process, and analyse major medical events (facilitating their preventability and predictability). Likewise, practitioners can grasp the news of each patient's case at any time and quickly develop a diagnosis and treatment plan (thus ensuring immediacy). On this point, Y Li and others, 'Literature Review on the Applications of Machine Learning and Blockchain Technology in Smart Healthcare Industry: A Bibliometric Analysis' (2021) J. HEALTCARE ENG.

Moreover, practitioners can access the medical system anywhere to request images and diagnoses of a patient that are, therefore, "readable" in any hospital through the medical network (in other words, an integral interconnection).[24]

It is worth noting that patient data is held by many different companies[25] and with the advent of the Internet of Things, the quality and quantity of information collected, stored, and provided will constantly increase. [26] Following in this vein, blockchain could lend its support to the aim of protecting users from privacy issues, 'providing also the way to have a unified and more efficient register for the costumers'.[27]

From a practical point of view, such a technological advance would make it possible to register two categories of data: (i) "on-chain" stored directly on the blockchain; (ii) and "off-chain" catalogued in the register through connections 'that act as a pointer to information stored in distinct, traditional databases'.[28]

The storage of medical information directly on the distributed ledger ensures that it is adequately protected by its own structure and is immediately visible to all those with specific authorisation to access the chain.[29]

Given these premises, the positive effects of such a system are innumerable. Consider the case in which a healthcare facility decides to use the blockchain; when an operator visits a patient, he creates an electronic medical record and thus sets up a new block in the chain. Every time the patient carries out examinations or routine checks, his or her file is updated, by means of a new block – which contains both the last report produced and the previous documents[30] – which, in turn, is transmitted to all the nodes.[31]

In this perspective, therefore, the mechanism of consent of the various nodes (via computer) of the chain just described represents a guarantee of transparency, through a safer and more efficient management of patients, medical records and the health data associated with them, as part of a sharable and immutable database that can be freely consulted by medical personnel -

---

[24] *Ibid*. Through the network, using portable mobile devices, medical personnel can constantly perceive, process, and analyse major medical events (facilitating their preventability and predictability). Likewise, practitioners can grasp information of each patient's case at any time and quickly develop a diagnosis and treatment plan (thus ensuring immediacy). Moreover, the medical staff can access the medical system anywhere to request images and diagnoses of a patient that are, therefore, available in any hospital through the medical network (in other words, an integral interconnection).

[25] D Nancy Kirupanithi, A Antonidoss, 'Analyzing the Cost Efficiency Using Attribute Based Encryption on Medical Blockchain Platform' (2020) 11 INT. J. ELECTR. ENG. TECHNOL., 396.

[26] On the role of IoT in healthcare system, N Neranjan Thilakarathne, 'The Role of the Internet of Things in Health Care: A Systematic and Comprehensive Study' (2020) 10 INT. J. ENG. MANAG. TECHNOL.

[27] MN Weldon, R Epstein, 'Beyond Bitcoin: Leveraging Blockchain to Benefit Business and Society' (2019) TRANSACTIONS, 863.

[28] Deborah and others, 'Blockchain: A Possible Alternative to Achieving Health Information Exchange (HIE)' (n 21) 162.

[29] R Krawiec and others, *Blockchain: Opportunities for Health Care*, (Deloitte 2016).

[30] Neranjan Thilakarathne, 'The Role of the Internet of Things in Health Care: A Systematic and Comprehensive Study' (n 26) 147-148.

[31] Deborah and others, 'Blockchain: A Possible Alternative to Achieving Health Information Exchange (HIE)' (n 21) 161.

clearly where all the characteristics of the case allow for respect of patient privacy.[32]

Thanks to the immutability of blockchain, as already mentioned, tampering would not be allowed (*rectius*, it would in fact be extremely unfeasible).[33] Unlike traditional databases, in fact, which rely on a centralised server, the use of a distributed system would allow the exchange of information among peers and with higher levels of security.[34]

In addition, a further advantage of medical records based on such a technological system is the possibility of improving interoperability between clinics, hospitals, and other healthcare providers.[35]

The information recorded on the public ledger could be widely accessible through private key systems, allowing patients to exchange their data much more easily with healthcare organisations.[36]

In this vein, technological differences in storage systems often make it difficult to share documents between organisations. Blockchains, conversely, would solve this problem by allowing authorised parties to access a unified database of medical records or even pharmaceutical distribution records.[37]

This would bring other "collateral" advantages affecting: (i) more effective management of the supply chain, (ii) protection from insurance frauds, (iii) clinical trials.[38]

Therefore, the advantage of having at disposal, in any health facility, the entire medical history of a citizen who, at that moment, needs treatment or assistance, re-proposes the need to build and constantly update a huge database whose information must also be treated in respect of privacy, regulated by the General Data Protection Regulation (GDPR) – which will be

---

[32] Borroni, 'Blockchain: Uses and Potential Value' (n 7) 41-42. The blockchain, moreover, should also facilitate the adoption of an Electronic Health Record (EER) since, as of today, for the same patient polyclinics, doctor's offices, hospital companies, individual doctors – each with their own management software – create several files that are often disconnected and the data are, therefore, often incomplete, and difficult to update. Although the analysis of the blockchain-privacy pair will be dealt with extensively in the last chapter, as far as privacy in healthcare is concerned, see, *ex multis*, JL Fernández-Alemán and others, 'Security and privacy in electronic health records: A systematic literature review' (2013) J. BIOMED. INFORM., 541–562.

[33] Deborah and others, 'Blockchain: A Possible Alternative to Achieving Health Information Exchange (HIE)' (n 21) 159. In this context, it is very important to ensure the integrity and validity of patient records. Furthermore, the use of algorithms to encrypt the data stored on the blockchain ensures that it can only be decrypted by users with legitimate data access permissions, thus improving data security and privacy. Furthermore, since the identities of clients in a blockchain are pseudonymised using cryptographic keys, patient health information can be shared between healthcare stakeholders without exposing patients' identities. See, on this point, also C Agbo and others, 'Blockchain Technology in Healthcare: A Systematic Review' (2019) HEALTHCARE, 56.

[34] Neranjan Thilakarathne, 'The Role of the Internet of Things in Health Care: A Systematic and Comprehensive Study' (n 26) 148.

[35] Deborah and others, 'Blockchain: A Possible Alternative to Achieving Health Information Exchange (HIE)' (n 21) 161-162.

[36] *Ibid*.

[37] Agbo and others, 'Blockchain Technology in Healthcare: A Systematic Review' (n 33) 56-57.

[38] A Deborah and others, 'Blockchain: A Possible Alternative to Achieving Health Information Exchange (HIE)' (n 21) 162.

discussed in detail in the last paragraph.

Regarding the handling of information in compliance with the GDPR, briefly, the flexibility in reading the blockchain will undoubtedly make it possible to provide for authorisations, manageable by the patient, in cases where consultation does not take place directly by healthcare facilities – as, for example, in the case of the pharmacy for checking the drugs to be purchased.[39]

It is desirable, therefore, to use "free" – permissioned – blockchains, to avoid that sensitive patient data can be freely consulted by persons who do not belong to the circle of insiders and processed unlawfully.[40]

In this way, GDPR compliance could be achieved where the blockchain is private and legitimised, *i.e.*, where all nodes in the network are known to each other and have the appropriate authorisation to view and add further blocks.[41]

3. Different types of blockchain.

What has been said so far shows that, depending on the objective to be pursued, various technological models may be applicable.

DLTs, in fact, are different from one another and, therefore, recourse to the term blockchain may be generic and misleading, since it is necessary to distinguish, as far as health issues are concerned, at least two main types: those that are permissionless and those that are permissioned[42] – there are, then, others, including hybrid or consortium ones; however, for the purpose of this discussion it will be sufficient to analyse only the first two types.

In particular, whether the aim is to increase the tools of research without any limits or conditions, the use of an open system (permissionless) would undoubtedly be preferable, given the intrinsic advantage of decentralisation and the objective of guaranteeing anyone the possibility of viewing the

[39] Fernández-Alemán and others, 'Security and privacy in electronic health records: A systematic literature review' (n 32) 541-562.

[40] R El Ghazzar, K Stendal, 'Blockchain in Health Care: Hope or Hype?' (2020) J. MED. INTERNET RES., 31-33. In this regard, '[a] proposed workaround is to store the patient data off-chain and have the pseudonym codes stored on-chain'. *Ibid.* See also, Agbo and others, 'Blockchain Technology in Healthcare: A Systematic Review' (n 33) 56; AA Vazirani and others, 'Implementing Blockchains for Efficient Health Care: Systematic Review' (2019) J. MED. INTERNET RES. However, 'this implies that the pseudonym code and any transaction records on the patient data that are stored on-chain would still be existent even after deleting the patient data that were stored off-chain. To reverse the immutability of blockchain, a proof-of-concept prototype for a "forgetting blockchain" was proposed to delete old data from private permissioned blockchains; however, the prototype still has limitations to address'. *Ibid.*

[41] Deborah and others, 'Blockchain: A Possible Alternative to Achieving Health Information Exchange (HIE)' (n 21) 163-164. The distributed register makes it difficult for data subjects, such as patients or providers, to exercise their rights related to the behaviour of a data controller because there is no single data controller, such as an organisation, that acts as the "keeper" of the data, but rather network nodes that each contain a copy of the data. In the EU Data Protection Regulation, rights related to the behaviour of a data controller include the right to access one's personal data, to rectify it, to be informed about its processing, to object to its processing and to have it erased. See, on this point, also Vazirani and others, 'Implementing Blockchains for Efficient Health Care: Systematic Review' (n 40).

[42] Catelani, 'Nuove tecnologie e tutela del diritto della salute: potenzialità e limiti dell'uso della Blockchain' (n 1) 221.

information contained in the registry and contributing to its management and updating (the basis of the Proof-of-Work scheme on which most blockchains are based).[43]

Conversely, the closed (permissioned) model should be used if the goal is to guarantee the interest of the individual patient, the individual. Permissioned systems, in this sense, can be regarded in the same way as private networks, in which the availability of data depends on the agreement – or rather, consent – of several predefined servers. From an operational point of view, they require an organisation and governance structure with a specific concession to view the register and, usually, basic instructions to access it.[44] In this sense, the approval system is no longer entrusted to the totality of participants but, indeed, to a limited group of nodes, or a single node, with recognised authority (the so-called Proof-of-Authority scheme).[45]

At the end of the day, the technical avenues within the blockchain are different and can be used to facilitate health protection, privacy, research, and healthcare organisation. In such a scenario, it is up to the technicians to study the most effective one to pursue the set goals, but, specifically, it is up to the healthcare organisation to embrace the novelty of data collection.[46]

What emerges, however, from the studies that have been carried out is the

---

[43] M Liu and others, 'How Will Blockchain Technology Impact Auditing and Accounting? Permissionless vs. Permissioned Blockchain' (2019) 13 CURR. ISS. AUD., 4 ff.

[44] DA Zetzsche and others, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2017) U. ILL. L. REV., 1372.

[45] In this context, '[w]hen new records are added, the ledger's integrity is checked through a limited consensus process carried out by trusted actors'. M Fink, 'Blockchain: Regulating the Unknown', (2017) 19 GERMAN L. J., 670.

[46] On this point, Borroni, 'Gli obblighi a carico del personale e dei liberi professionisti che operano nella struttura (n 20) 67-74. It is prefigurable, *ictu oculi*, a positive obligation of *facere* on the part of the recipients of the same, burdening them with the duty to take part in the clinical risk prevention activities conducted in the facilities in which they serve. In particular, healthcare professionals are required to observe, in the performance of their services, a particularly qualified diligence, appropriate to the nature of the activity exercised (Article 1176, paragraph 2, of the Civil Code) and declined in terms of "expertise", in the sense of compliance with an "ideal" model of conduct that derives from the application of the knowledge and rules of technical-scientific experience proper to the *ars medica*, according to a variable standard in relation to the specific professional category. This perspective represents a significant step forward in the "balancing of burdens" on those involved in the exercise of the health profession and allows the Italian system to align itself with the evolved systems of risk prevention and management typical of foreign experiences, first and foremost that of the United States, following an imitative approach already adopted in other areas of law. As highlighted by G Alpa, 'La responsabilità medica' (1999) 21 *Rivista Italiana di Medicina Legale e del Diritto in campo sanitario*, 15 ff, a new paradigm has been created whereby the "patient monad" and the "healthcare monad" are set in opposition from a civil law perspective, the latter including the healthcare facility and the personnel and means at its disposal. Think of the use of algorithms to improve the collection and processing of personal data relating to the health of individuals, for diagnostic or scientific research purposes. For an analysis on the subject see U Ruffolo, 'L'Intelligenza artificiale in sanità: dispositivi medici, responsabilità e ''potenziamento''' (2021) GIUR. IT., 502 ff; G. Pascuzzi, *Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche* (Zanichelli 2020); P Guarda, '"Ok Google, am I sick?": Artificial Intelligence, E-Health, and Data Protection Regulation' (2019) 1 BIODIRITTO, 359 ff; G Finocchiaro, 'Intelligenza artificiale e diritto. Intelligenza artificiale e protezione dei dati personali' (2019) GIUR. IT., 1657 ff; G Pascuzzi and others, *Comparative Issues in the Governance of Research Biobanks. Property, Privacy, Intellectual Property, and the Role of Technology* (Springer 2013); U Izzo, P Guarda, 'Sanità elettronica, tutela dei dati personali e digital divide generazionale: ruolo e criticità giuridica della delega alla gestione dei servizi di sanità elettronica da parte dell'interessato' (2010) *Trento Law and Technology Research Group Research Papers*.

delays in the digitisation of health data of the patients, more than anything else because of justified fears related to the management of sensitive data, the leakage of which can be particularly detrimental to the rights of the citizens concerned, so that the need to combine both the interest in the circulation of data and the need to use techniques that guarantee privacy rights to the citizens is even more pressing, and in this perspective, precisely, blockchain may represent a viable solution.[47]

4. Health protection and data protection.

In the light of the conducted analysis, there are many points of interest involving the protection of personal data.

In the contemporary global scenario, the new dynamics of information collection and processing, the greater invasiveness of control over individuals, both by public and private entities, have led to an ever-increasing demand for protection.[48]

This discussion is of interest in relation to the regulation of the processing of so-called super-sensitive data, such as health data, since there is a need to define a reasonable balance between the right to health, which requires that the provision of services necessary to safeguard the health and physical integrity of the person concerned and of third parties should not be hindered, and an adequate maintenance of the guarantees prescribed to protect privacy.[49]

In the processing of health information, in particular, data protection provisions are normally 'supplemented by administrative laws that govern retention, resulting in different obligations and conservation timescales, deontological rules and sectoral norms. The scenario is characterized by the coexistence of normative sources and different actors, given a strong need for self-regulation'. [50] However, considering the sensitivity of the data to be

[47] Catelani, 'Nuove tecnologie e tutela del diritto della salute: potenzialità e limiti dell'uso della Blockchain' (n 1) 222-223.

[48] On this point, G Resta, 'Le persone e la famiglia. Le persone fisiche e i diritti della personalità', in G Alpa, G Resta, *Trattato di diritto civile*, directed by R. Sacco (Giappichelli 2019) 145 ff. The author privileges a "value-oriented" interpretation, considered the most appropriate line for dealing with issues concerning the person and personality rights. In this scenario, the globalisation of markets and the evolution of technologies constitute, for the authors, complex challenges to the role of law.

[49] Farina, 'Blockchain e tutela della salute: verso la riorganizzazione dei sistemi sanitari?' (n 4) 183. See, generally, on privacy and blockchain M Seghesio, 'Blockchain and Privacy', in Borroni, 'Blockchain: Uses and Potential Value' (n 7) 138 ff. In particular, in the current globalised panorama, the gravitational centre of gravity of the right to privacy is increasingly identified, rather than in the right to be "left alone", in the possibility of each subject to control the use of the information that concerns him or her and in considering the problems of privacy in the framework of the current organisation of power, of which the information infrastructure now represents one of the fundamental components. S Rodotà, 'Tecnologia e diritti (Zanichelli 1995) 19.

[50] M Arisi, P Guarda, 'Blockchain and eHealth: seeking compliance with the General Data Protection Regulation' (2020) BIOLAW J., 489. With regards to the italian context, see E Lamarque, 'Privacy e Salute', in G Losano (ed.), *La legge italiana sulla privacy - Un bilancio dei primi cinque anni*, (Cacucci 2001) 338-339. For

processed, Privacy and Data Protection are certainly key issues for the healthcare applications, eHealth requiring specific attention as it introduces new use-cases and vulnerabilities.[51]

The first aspect is related to data accessibility. In this perspective, it is reasonable to associate the increasing transparency of information with a decreasing respect for the right to privacy.[52]

In fact, the data contained within the blockchain registry are physiologically public; an aspect, this, that would seem to collide – at least *prima facie* – with the data processing rules provided for by European Regulation no. 679/2016 (GDPR).[53]

Transposing this assertion to the blockchain systems used, it is crucial to identify specific arrangements to ensure that access and processing activities are restricted and authorised only in favour of certain persons and in such a way as to enable the integrity of the entire database, also by means of appropriate security measures.[54]

From a different point of view, however, critical elements could be found in relation to the principle of information minimisation, which presupposes the definition of limited retention times. In fact, the data in the blockchain are stored indefinitely fulfilling the guarantees of certainty and verifiability over time, and once they become part of the chain, they are recorded permanently and unalterably within it.[55]

---

instance, Guidelines and Opinions by the Italian Data Protection Authority are fundamental to the interpretation of the legislative content; on this point see GM Riccio, 'Privacy e Dati sanitari', in F Cardarelli and others, *Il Codice dei dati personali - Temi e problemi* (Giuffrè 2004); G Finocchiaro, 'Privacy e protezione dei Dati personali – Strumenti Operativi' (Zanichelli 2012) 295-317.

[51] *Ibid*.

[52] Be permitted a reference to F Zambardino, 'La blockchain nel mercato del lavoro italiano con particolare enfasi sulla questione privacy e il rapporto con il General Data Protection Regulation' (2022) 3 TSL, 23-38.

[53] On the relationship between GDPR and data protection G Alpa, 'La "proprietà" dei dati personali, in Persona e mercato dei dati. Riflessioni sul GDPR', in N Zorzi Galgano (ed.) (Giuffrè 2019) 17 ff; G Finocchiaro, 'Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali' (Zanichelli 2017) 101 ff; L Bolognini and others, *Il Regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali* (Giuffrè 2016) 277 ff. Before the entry into force of the GDPR with particular reference to the processing of health data, 'the former Privacy Code (Legislative Decree 196/2003) provided that the same could be processed only with the consent of the person concerned and after authorization from the Guarantor (art. 26, paragraph 1). In other words, the consent of the interested party was given a central role as a legitimate prerequisite and condition of lawfulness of the processing of personal data. Therefore, the rule was that the personal data could be processed only with the consent of the person concerned and exceptions were provided for (and justified) only by the extraordinary nature of certain situations'. F Rosa, 'The use of it tools and artificial intelligence in the health sector: the patient as a vulnerable subject' (2020) 2 EJPLT, 225-226.

[54] AM Gambino, C Bomprezzi, 'Blockchain e protezione dei dati personali' (2019) DIR. INFOR., 620 ff. See for a general overview Arisi, Guarda, 'Blockchain and eHealth: seeking compliance with the General Data Protection Regulation' (n 50) 477-496; P Guarda, L Petrucci, 'Quando l'intelligenza artificiale parla: assistenti vocali e sanità digitale alla luce del nuovo regolamento generale in materia di protezione dei dati' (2020) BIOLAW J., 425-446.

[55] Farina, 'Blockchain e tutela della salute: verso la riorganizzazione dei sistemi sanitari?' (n 4) 184. In This would run the risk of, on the one hand, undermining the main rights of data subjects under Articles 15 to 22 of the European Regulation, such as the right to obtain the updating, rectification or integration of personal data concerning them, and, on the other hand, of rendering ineffective the requirements of deletion, anonymisation or destruction of data in the event of cessation of processing.

The primary need that remains is to find the right balance between the use of DLTs – in all spheres, but specifically the one under analysis – and the protection of personal data, so that the principles of "data protection by design and by default" can concretely become the necessary starting point for the development of *secundum legem* technological solutions.[56]

It is possible, therefore, to state that blockchain can be compatible with the protection of health data; in light of the technical-operational features described, it would seem to be feared that it might even be possible to fulfil certain obligations to protect the information contained in the registry, in the event that one opts for so-called "permissioned" systems – *i.e.* private ones, as discussed in the preceding paragraph.[57]

Moreover, the use of this technology is fully in line with the recent positions of the European Parliament, summarised in a Resolution of 3 October 2018.[58]

Firstly, the importance and applicative instrumentality of blockchain and, more generally, of any distributed system is grasped; secondly, among the application profiles examined, particular attention is paid to the healthcare sector. The latter, according to the Resolution, could benefit greatly from the use of DLT, in terms of greater control by citizens over their own data, as the maximum expression of their deterministic power, being able to choose which information to share; such a dialogic contribution would translate into increasing levels of transparency, while considering the need to safeguard the confidentiality of the data processed.[59]

At the same time, it is also possible to identify several critical profiles that collide with the protection of privacy. Starting from the assumption that, in the field of DLTs, data are considered pseudonymous and not anonymous, they require the adoption of the measures established by the GDPR.[60]

---

[56] In such a scenario, Article 25 of the GDPR on data protection by design requires the data controller to implement appropriate technical and organisational measures aimed at effectively implementing data protection principles, such as minimisation, and at incorporating the necessary safeguards into the processing to meet the requirements of this Regulation and to protect the rights of data subjects. Gambino, Bomprezzi, 'Blockchain e protezione dei dati personali'(N 54) 624-625. In particular, the GDPR entrusts the data controller with the choice of the most suitable solutions for achieving the objective of risk management, arising from the processing of personal data, and stipulates that he or she will be held accountable if problems arise. Be permitted a reference to F Zambardino, 'La blockchain e la protezione dei dati personali: una tecnologia privacy compliant by design?' (2022) 2 EJPLT, 136-152. See also R Carleo, Il principio di accountability nel GDPR: dalla regola alla auto-regolazione' (2021) NUOVO DIR. CIV., 366 ff; G Comandè, 'Responsabilità e accountability nell'era dell'Intelligenza Artificiale', in F Di Ciommo, O Troiano, *Giurisprudenza e Autorità indipendenti nell'epoca del diritto liquido. Studi in onore di Roberto Pardolesi* (La Tribuna 2018) 1010 ff; M. Trapani, 'GDPR e Intelligenza Artificiale: i primi passi tra governance, privacy, trasparenza e accountability', in A Mantelero, D Poletti (eds.), *Regolare la tecnologia: il Regolamento UE 2016/679 e la protezione dei dati personali* (Pisa University Press 2018).

[57] Be permitted reference to Zambardino, 'La blockchain e la protezione dei dati personali: una tecnologia privacy compliant by design? (N 56) 136-152.

[58] European Parliament resolution of 3 October 2018 on distributed ledger and blockchain technologies: building trust through disintermediation (2017/2772(RSP)).

[59] Farina, 'Blockchain e tutela della salute: verso la riorganizzazione dei sistemi sanitari?' (n 4) 186.

[60] In particular, the aspect of pseudonymisation of personal data (*i.e.,* 'data can no longer be attributed to a specific individual without the use of additional information' Art. 4, no. 5, GDPR) is specifically regulated by

One of these is, definitely, the governance issue. In order to 'implement data protection roles in a blockchain healthcare project may be challenging because definition of data protection roles in the sector can be complex per se and has been debated through timeì.[61] For instance, with reference to the management of health records, exchange of data takes place in diverse environments, presenting different structures according to more than one organizational practice; on this matter, digitalization is ultimately contributing to create a new scenario:[62] the possibility 'to build a blockchain that can mirror the logic of this complex data exchange represents a great opportunity'.[63]

However, the most challenging critical element is that relating to the difficulties inherent in the proper exercise of the rights of the protected subject, placing particular emphasis on the right to be forgotten, which is, moreover, the subject of recent and further hermeneutic discussions.[64]

The last valuable aspect of the Resolution can be found in the identification of the competent Authority to provide a more precise framework on the point: indeed, from the analysis of Article 32, the Parliament invites the European Commission and the European Data Protection Supervisor to provide further guidance on the point.

A dynamic landscape is therefore foreshadowed, disseminated by soft law activities and collaborative relations between the network of competent independent authorities.[65]

---

the GDPR and is subject to the condition that the additional information is "stored separately" and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person.

[61] Arisi, Guarda, 'Blockchain and eHealth: seeking compliance with the General Data Protection Regulation' (n 50) 494. See also, more generally, P Guarda, *Fascicolo Sanitario elettronico e protezione dei dati personali* (Università degli Studi di Trento 2011) 106.

[62] P Guarda, 'I Dati sanitari', in V Cuffaro and others, *I dati personali nel diritto europeo* (Giuffrè 2019) 609-617.

[63] Arisi, Guarda, 'Blockchain and eHealth: seeking compliance with the General Data Protection Regulation' (n 50) 494.

[64] The relationship between the right to be forgotten and the right to report news was the subject of a question referred to the United Sections of the Supreme Court of Cassation, which ruled in Judgment No. 19681 of 22 July 2019. On that occasion, the United Sections reiterated the constitutional relevance of both the right to report news and the right to oblivion, specifying that when a piece of news, previously disseminated in the legitimate exercise of the right to report news, is disseminated again, the right of the person concerned to maintain anonymity over his or her personal identity prevails. For more details see the recent contribution by F Balducci Romano, 'La Corte di giustizia 'resetta' il diritto all'oblio' (2020) FEDERALISMI. For an examination of the legal concept of forgetting, see A Palmieri, R Pardolesi, 'Polarità estreme: oblio e archivi digitali' (2020) 1 FORO IT., 1570 (comment to Cass., sez. I, 27 marzo 2020, n. 7559); R Pardolesi, 'Oblio e anonimato storiografico: «usque tandem...»?' (2019) 1 FORO IT., 3082 (comment to Cass., sez. un., 22 luglio 2019, n. 19681); S Martinelli, 'Diritto all'oblio e motori di ricerca: il bilanciamento tra memoria e oblio in Internet e le problematiche poste dalla de-indicizzazione' (2017) DIR. INFOR.; R Pardolesi, 'Diritto all'oblio, cronaca in libertà vigilata e memoria storica a rischio di soppressione' (2016) 1 FORO IT., 2734 (comment to Cass., sez. I, 24 giugno 2016, n. 13161).

[65] Farina, 'Blockchain e tutela della salute: verso la riorganizzazione dei sistemi sanitari?' (n 4) 186-187.

5. Blockchain and telemedicine.

One of the most promising uses of blockchain in the healthcare sector is potentially that related to telemedicine, which makes use of innovative and in some ways still developing technologies to provide care services in contexts of physical distance between the actors involved.[66]

As is well known, telemedicine makes use of Information and Communication Technologies (ICT) to facilitate the secure sharing of medical data in any digital form, useful for prevention, diagnosis, treatment, and examination activities.[67]

Although they can be compared to traditional healthcare services and although they must respect all their rights and obligations, telemedicine services do not totally replace them, but their integration guarantees statistically superior results.[68]

Specifically, the adoption of telemedicine systems in the healthcare sector brings about new dynamics of cooperation between patients and operators, contributing to a concomitant improvement in the services offered. Firstly, in terms of quality of care, since patients' parameters can be constantly monitored remotely; secondly, greater coverage, understood as agility in providing healthcare to individuals living in areas that are difficult to access or distant from hospital facilities; thirdly, greater effectiveness and efficiency, through constant interaction between the various actors involved; and finally, also in economic terms, the optimisation of resources brings as a first consequence a rationalisation of social-health processes, allowing a significant reduction in costs.[69]

Amongst the various positive elements that have been outlined in the previous paragraphs, there also remains the risk of a possible data breach and, consequently, fears in terms of patient privacy. Indeed, centralised systems are vulnerable to external attacks by hackers and malicious users; this represents an element of mistrust towards remote services that often leads to a preference for traditional methods.[70]

---

[66] For a general discussion on the subject, see, NM Hjelm, 'Benefits and drawbacks of telemedicine' (2005) J. TELEMED. TELECARE, 60-70.

[67] Among the first in Italian doctrine U Izzo, 'Medicina e diritto nell'era digitale: i problemi giuridici della cibermedicina' (2000) DANNO RESP., 807 ff. It is clear that telemedicine involves at the same time different disciplines: telecommunications, information technology, and medicine. Telemedicine is seen as a rib of the Anglo-Saxon concept of "telehealth" and "telecare", which lead to a systematic refurbishing of the health system, from the organization and management to the training and education of patients and medical operators. Blockchain technology ensures then a secure interchange of data, imageries, and papers among the patients and medical staff, prevention, analysis, cure, and monitoring can be done without physical presence of the doctor or at the healthcare facilities.

[68] K Griggs and others, 'Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring' (2018) J. MED. SYST'S, 42 ff.

[69] E Funk '*Blockchain Technology: A Data Framework to Improve Validity, Trust, and Accountability of Information Exchange in Health Professions Education* (2019) 93 J. ASS. AM. MED. COLL., 93 ff.

[70] Griggs and others, 'Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring' (n 68) 42 ss.

The effectiveness of virtual care and health monitoring depends on the integrity of Electronic Health Records (EHRs), which include a patient's medical history, diagnosis, medication, and treatment plans.[71] EHRs contain highly sensitive and private information, which needs to be shared securely between facilities – hospitals, pharmacies, and health authorities – to keep medical data up to date.[72]

The introduction of blockchain in this context would foreshadow a strengthening of trust, given the lack of intermediaries inherent in this technology. By means of this system, the management of consent is secured and protected by several "peers" belonging to different and "distributed" participating organisations.[73]

A further issue is the difficulty for healthcare organisations to manage the quantity of patient records due to limited interoperability.[74] To overcome this impasse, blockchain provides a single, consistent view of electronic patient records for all participating stakeholders. The visibility and transparency of information allows participating organisations to trace a patient's medical history to propose appropriate treatment.[75]

Virtual healthcare systems based on online advice, in addition, require the practitioner to enter patient's data into the registry sharing the prescription of drugs with pharmacies. Through hash functions, the blockchain can help eliminate potential prescription errors.[76] Registered pharmacists can access prescriptions to verify, prepare and send drugs to patients. And, in this sense, transparency and traceability can also allow patients and doctors to verify the actual "originality" of the drug by analysing its provenance.[77]

---

[71] In Italy, Article 12 of the decree law no. 179/2012 regulates the electronic health record and surveillance systems in the health sector, in which the concept of the health record is defined, but more than anything else the underlying objectives are identified, including the reference to guaranteeing health, facilitating scientific research and purely organisational profiles, such as health planning, verification of the quality of care and evaluation of health care. Guarda, *Fascicolo Sanitario elettronico e protezione dei dati personali* (n 61) 106 ff.

[72] The legal definition of the EHRs in the regulatory context of personal data protection cannot but reflect a vision of care that the National Health System as a whole (a system in which public and private subjects take their place with differentiated, but increasingly integrated roles and responsibilities) intends to pursue, in the awareness that information assumes, today more than ever, a key role in any process traceable to the ideal objective of protecting the health of the citizen/patient/interested party. Pascuzzi, *Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche* (n 46) 86.

[73] P Genestier and others, 'Blockchain for consent management in the ehealth environment: a nugget for privacy and security challenges' (2017) J. INT. SOC. TELEMED. EHEALTH., 5 ff.

[74] Arisi, Guarda, 'Blockchain and eHealth: seeking compliance with the General Data Protection Regulation' (n 50) 489. The authors state that '[t]he need for interoperability, selective access and security and integrity of data are an essential feature of this sector and this is why several blockchain-based projects can be found, but the reference is especially to the opportunities related to private and permissioned blockchains, which ensure confidentiality of the data'.

[75] RW Ahmad and others, 'The role of blockchain technology in telehealth and telemedicine' (2021) INT. J. MED. INFORM., 6.

[76] Y El-Miedany, 'Telehealth and telemedicine: how the digital era is changing standard health care' (2017) SMART HOMECARE TECHNOL. TELEHEALTH., 45-46.

[77] Ahmad and others, 'The role of blockchain technology in telehealth and telemedicine' (n 75) 7.

Finally, a side advantage can also be found regarding insurance. For example, in the case of insurance fraud (think of the submission of an incorrect claim for treatment costs to an insurance company), the administrative costs of establishing the veracity of the information provided are high. Blockchain technology can help both insurers, in terms of minimising insurance fraud (by authorising them to access a patient's medical record), and policyholders (*i.e.,* patients) who can be incentivised to provide consent to use their medical data for insurance purposes. [78] The growing need to collect information on customers for the purpose of tailoring personalised products on them, calibrated to risks monitored either through digital devices or diagnostic tools, is, in a way, contextualised.

However, it should be emphasised that telemedicine systems, to function properly, require close coordination between the actors involved in healthcare processes, to maintain a consistent and up-to-date patient history and reduce diagnostic errors.[79]

Conclusive remarks.

The application of blockchain in healthcare has still encountered many difficulties, especially regarding privacy, data management and control, given the resistance of this sector to embrace new technologies or change its organisational patterns.

This is true if one considers the internal structure of DLTs, based on the building block. The medical history is permanently compiled and available to all practitioners wherever they are, supporting the necessary procedures to efficiently activate mechanisms such as telemedicine and remote assistance.

As far as increasing security is concerned, it is worth remembering that whenever data is entered by a node, it cannot be damaged, altered or deleted and, at the same time, the patient can control who has entered a piece of data and who has read it, with a mechanism of maximum transparency.

From this point of view, this can be advantageous in reducing the liability of doctors and healthcare facilities, especially if this is linked to specific guidelines to be followed.[80]

---

[78] *Ibid.*

[79] Griggs and others, 'Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring' (n 68) 42 ff. On the matter see also F Cerea, 'Intelligenza artificiale a servizio dei pazienti per il contrasto a CoViD-19' (2020) NUOVA GIUR. CIV. COMM., 45 ff.

[80] On the matter, PG Monateri, 'La responsabilità civile', in *Trattato di diritto civile*, directed by R. Sacco (Giappichelli 1998) 753 ff. The author states that just as medical liability constituted a subsystem of the latter within civil liability, so too within contractual liability it nevertheless continues to present profiles of marked peculiarity. However, since the liability approach necessarily implies that the damage has occurred, the perspective to be taken, especially in the health sector, is that of security, including cyber security, which is the way to provide manufacturers of digital health solutions, as well as health professionals and users of these solutions, with rules, protocols and tools to prevent and reduce the risks that these solutions may present. G Capilli, 'Innovazione tecnologica e responsabilità: un breve sguardo alla "sanità mobile"

The implications of using blockchain are manifold and vary depending on the perspective of the users (be they patients, doctors, or the facilities themselves); at present, however, understanding of the potential of the technology (and blockchain in particular) is still "opaque". Involvement in medical insurance, in emergency cases, in product testing, in monitoring through statistical tools and mathematical or geometric graphs, are just some of the areas where the investigation is at least promising.[81]

(mHealth)' (2023) 1 EJPLT, 69-70. Legal scholars, in analyzing liability arising from the use of technology – *latu sensu* – in the medical field, have made reference to the standard provided by the Article 2050 of the Italian Civil Code related the assumption of liability for individuals who engage in activities that are particularly dangerous and potentially offensive to third parties. The activity taken into consideration is that which, by its nature, or the nature of the means employed, is defined as "dangerous". See P Perlingieri, 'Responsabilità civile e robotica medica' (2020) TECN. DIR., 165 ff.

[81] The consequences and the possible effects in the hiring process are manifold if it considered the power of an employer that could have potentially access to a candidate's health information and verify chronic pathologies, some latent physical difficulties, the days and places in which treatments took place and visits, any vaccinations, the number of days of illness and thus drive one's choice with an impact that ranges from contracts in the world of sport to more sedentary jobs. Indirectly, then, this availability of information would also lead to indirect control of the conduct of the doctors and eventual medical malpractice.