Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD)
14(3):300-312, setembro-dezembro 2022
Unisinos - doi: 10.4013/rechtd.2022.143.01

Cybersecurity, privacy, and health data protection in the digital strategy of the European Union

Cibersegurança, privacidade e proteção de dados de saúde na estratégia digital da União Europeia

Carlo Botrugno[1]
Università degli studi di Firenze, UNIFI/Italia
carlo.botrugno@unifi.it

Abstract

Contemporary societies increasingly rely on the opportunities created by technologies that make possible the production, collection, processing, and reuse of huge datasets to obtain inferences that can be used in the most disparate fields. Among these, healthcare stands out in importance since in medical practice a considerable series of personal information is exchanged and shared. The protection needs of the individual sphere in the healthcare sector acquire a specific scope with reference to the use of information and communication technologies, which allow patients and healthcare professionals to communicate, or the latter among them, in view of the achievement of a series of goals that pertain to the diagnosis, prevention, monitoring, rehabilitation and treatment of an increasingly large number of diseases. In such a context, this works aims at proving a synthetic overview on the whole architecture adopted by the European Union in the field of cybersecurity, privacy, and health data protection, which appears fundamental for guaranteeing the fundamental rights of European citizens but also to deal with the challenges posed by the digital transition of contemporary societies.

Keywords: cybersecurity, privacy, data protection, health data, EU digital strategy, information, and communication technologies.

[1] Researcher at Department of Legal Sciences, University of Florence. Coordinator of the Research Unit on Everyday Bioethics and Ethics of Science. L'Altro Diritto Inter-university Research Centre. Università degli Studi di Firenze, Via delle Pandette, 35, CEP 50127, Florence, Toscana, Italy.

Resumo

As sociedades contemporâneas contam cada vez mais com oportunidades criadas por tecnologias que possibilitam a produção, coleta, processamento e reutilização de enormes conjuntos de dados para a obtenção de inferências que podem ser utilizadas nas mais diversas áreas. Dentre elas, a saúde se destaca em importância, pois na prática médica uma série considerável de informações pessoais é trocada e compartilhada. As necessidades de proteção da esfera individual no setor da saúde adquirem um âmbito específico no que se refere à utilização das tecnologias de informação e comunicação, permitindo a comunicação entre doentes e profissionais de saúde, ou estes entre si, tendo em vista a concretização de uma série de objetivos que dizem respeito ao diagnóstico, prevenção, acompanhamento, reabilitação e tratamento de um número cada vez maior de doenças. Neste contexto, este trabalho pretende fornecer uma visão sintética sobre toda a arquitetura adotada pela União Europeia no domínio da cibersegurança, privacidade, e proteção de dados pessoais e não pessoais de saúde, que se afigura fundamental para garantir os direitos fundamentais dos cidadãos europeus, mas também para lidar com os desafios colocados pela transição digital das sociedades contemporâneas.

Palavras-chave: cibersegurança, privacidade, proteção de dados, dados de saúde, estratégia digital da UE, tecnologias de informação e comunicação.

Introduction

Contemporary societies increasingly rely on the opportunities created by technologies that make possible the production, collection, processing, and reuse of huge datasets to obtain inferences that can be used in the most disparate fields. Among these, healthcare stands out in importance since in medical practice a considerable series of personal information is exchanged and shared. This exchange can take place through complex technology systems, or, more simply, through commonly used communication tools such as the exchange of e-mails and other written messages. This information not only allows the direct identification of patients but also to access their health conditions, which is why it belongs to the category of so-called "sensitive data", together with any other information from which it is possible to infer sexual orientation, racial or ethnic origin, religious and philosophical beliefs, political opinions, trade union membership of individuals. As we will see, this information must be the object of "enhanced protection" since it concerns the most intimate part of the person in his body and in his deepest psychological convictions.

The protection needs of the individual sphere in the healthcare sector acquire a specific scope with reference to the use of information and communication technologies (hereinafter ICTs), which allow patients and healthcare professionals to communicate, or the latter among them, in view of the achievement of a series of goals that pertain to the diagnosis, prevention, monitoring, rehabilitation and treatment of an increasingly large number of pathologies (World Health Organization, 2010; Botrugno, 2018). The advent of the COVID-19 pandemic

has seen an unusual acceleration of digitization processes that have contributed to the consolidation of what can be defined as "informational medicine", a paradigm that is ever less based on physical contact between doctors and patients and, more generally, on the sensory faculties of the latter, to favour the collection and analysis of data taken from the human body (Lupton, 2013). Data, therefore, not only represent the "raw material" on which informational medicine feeds, but also the final result of the large-scale use of health services mediated by ICTs.

Among the main topics of the debate concerning the ethical-juridical implications deriving from the diffusion of ICTs in healthcare, there is the risk associated with the possibility of tracing the health conditions of patients, which implies the collection of a series of information and data of a sensitive nature, the treatment of which can prove to be a harbinger of pitfalls. This is demonstrated by the growing violations of privacy also in the healthcare sector (Liu *et al*., 2018; Verizon, 2018). It is no coincidence that legal doctrine has made considerable efforts to try to illustrate the critical profiles inherent in the legitimacy of data collection and processing activities in the health sector (Comandé, 2019; Pedrazzi, 2019). As we will see in the continuation of this work, the protection of health data is grafted onto a terrain that appears to be central to the whole architecture adopted by the European Union (EU) in the field of cybersecurity, privacy, circulation, and re-use of personal and non-personal data. Such architecture appears fundamental for guaranteeing the fundamental rights of European citizens but also to deal with the challenges posed by the digital transition of contemporary societies.

ICTs and health data in the EU Digital Strategy

Since the early 2000s, the European Commission has launched a process aimed at supporting Member States in the process of introducing ICT-mediated health services into their health systems. The first stage of this process can coincide with the issue of the e-Health Action Plan of 2004 (European Commission, 2004) which in the following years flows into the broader Policy for Aging Well With ICTs, developed under the aegis of the Digital Single Market, to then land in the most recent and all-encompassing Digital Strategy for the EU. The latter expressly includes a European Data Strategy which outlines a global approach whose ultimate goal is to "increase the use and demand for data and data-based products and services across the single market" (European Commission, 2020). Within the latter, data represents the lifeblood of economic development as they form "the basis for many new products and services, driving productivity and resource efficiency gains across all sectors of the economy, allowing for more personalised products and services and enabling better policy making and upgrading government services" (European Commission, 2020, p. 2). More specifically, the objective pursued by the European Union in this context is that of the creation of a single European data space or "a genuine single market for data, open to data from across the world – where personal as well as non-personal data, including sensitive business data, are secure and businesses also have easy access to an almost infinite amount of high-quality

industrial data, boosting growth and creating value, while minimising the human carbon and environmental footprint" (European Commission, 2020, p. 4).

With more specific reference to the healthcare sector, the European Commission had already expressed its orientation through Communication No. 233/2018, relating to the "digital transformation of health and assistance in the digital single market, the empowerment of citizens and the creation of a healthier society". In that context, the Commission had repeatedly highlighted the advantages deriving from the digitization of assistance, including the possibility of increasing the well-being of millions of citizens and radically changing how health and welfare services are provided to patients (European Commission, 2018). From the perspective of the European Commission, the potential of ICT in healthcare becomes even more evident when one considers that healthcare systems in industrialized countries are facing multiple challenges including an aging population, increasing comorbidities, the scarcity of healthcare personnel, the increase in non-communicable diseases and the re-emergence of infectious ones. In this context, the penetration of digital healthcare services into routine practice would make it possible to promote continuity of care, improve health conditions and the overall well-being of the population, also in the workplace, but also to "support the reform of health systems and their transition to new care models, centred on people's needs and enable a shift from hospital-centred systems to more community-based and integrated care structures" (European Commission, 2018, p. 1).

In such a context, therefore, it is evident that health data represent the fulcrum of a process that is intended not only to improve the accessibility and efficiency of health systems but also to fuel the broader digital transformation of European society. In the analysis offered by the Commission in Communication No. 233/2018, however, it clearly emerges how the fragmentation of the services market in this sector, combined with problems relating to the interoperability of health data, has made it impossible to achieve the objective of an "integrated approach" to the prevention of disease and the predisposition of the best possible response for the population of EU Member States. From this awareness arises the need to create a "European Health Data Space", which has taken the form of a proposal for a Regulation[2] (European Parliament, 2022) which provides provisions, common rules and practices, infrastructures and a governance framework for the primary and secondary use of electronic health data (Art. 1, paragraph 1) and which sets itself ambitious objectives, namely strengthening the rights of natural persons in relation to the availability and control of their electronic health data; establishing rules for the placing on the market, making available on the market or putting into service of electronic health record systems in the EU; establishing rules and mechanisms to support the secondary use of electronic health data; setting up a cross-border infrastructure enabling primary use of electronic health data across the EU; establishing a cross-border infrastructure for the secondary use of electronic health data (Art. 1, paragraph 2).

[2] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0001.02/DOC_1&form at=PDF

The dynamic notion of protection introduced by the EU General Data Protection Regulation

The EU has redesigned its personal data protection system through the issuance of Regulation No. 2016/679 (briefly GDPR), which in addition to introducing rules relating to the protection of natural persons with regard to the processing of personal data, also provides for rules relating to the free circulation of such data (art. 1). The GDPR remarks the emphasis on the free circulation of personal data within the EU, emphasizing that this cannot be limited or prohibited for reasons relating to the protection of natural persons with regard to the processing of personal data (art. 1, paragraph 3). As has been highlighted by the legal doctrine in this regard, the provisions of the GDPR "have nothing to do with confidentiality in the strict sense" but rather pertain "to the regime of circulation of information, in part typical of other sectors and matters, such as the market of competition on information and access to information" (Finocchiaro, 2018, p. 896).

Since its *incipit*, therefore, the GDPR makes clear the indissoluble combination between the protection of personal data and the free circulation of the same in the EU area, a sign of "detachment" by the European legislator "from the substantially static conception of the right to respect for private life, in which an eminently negative protection was sufficient, consisting in the power to exclude the interference of others" (Colapietro, 2018, p. 4). As highlighted by the doctrine, in fact, the idea of protection exclusively aimed at the "natural person" has become obsolete within contemporary societies, the functioning of which has instead made it necessary to adopt a "dynamic" conception of protection of data, i.e. a protection that "follows the data in the moment of their circulation" (Colapietro, 2018, p. 4.). This corresponds to the transition from a "one-way model", in which the flow of data mainly occurred from the interested party to the data controller, to one of "sharing and co-management" of data and information which appear to be "destined from the outset to a global circulation" (Finocchiaro, 2017, p. 1).

On the other hand, the transition from the *habeas corpus*, to the *habeas data* (Colapietro, 2018, p. 14), was sealed by the choice to provide a right to data protection alongside the more classic right to private and family life (respectively, articles 7 and 8 of the EU Charter of Fundamental Rights). This choice would have contributed to transforming the approach in this matter from market-driven to fundamental rights-oriented (Bassini, 2016, p. 588).

A further element to consider is the new definition of "personal data" adopted within the GDPR, a very broad definition – according to some, so broad as to be potentially all-encompassing, with the risk of frustrating the same protection provided by the new regulatory system (Purtova, 2018). Based on this new definition offered by Art. 4 of the Regulation, any information concerning an identified or identifiable natural person represents personal data. More specifically, such natural persons are considered identifiable when they can be identified, directly or indirectly, having particular regard to "an identifier such as a name, an identification number, location data, an online identifier or to one or more factors

specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (art. 4, GDPR).

On the one hand, the breadth of this definition could be ascribed to the desire to envisage a flexible category, capable of including new cases that may arise in the future as a result of technological evolution. On the other, some have underlined that this choice must be interpreted as a sign of the transposition of some orientations that emerged within the US doctrine on the matter, according to which the dichotomy between personal data and anonymous data must be seen as "outdated" (Colapietro, 2018, p. 15). For this work, it is worth emphasizing that these orientations would acknowledge the failure of the anonymization procedures, and in particular from the awareness that the distinction between personal data and anonymous data is no longer adequate in the light of the needs conflicting data protection factors and circulation of the latter (Ducato, 2016, p. 164). This would also explain the choice made by the EU legislator to foresee preventive measures aimed at mitigating the risk of privacy violation (Colapietro, 2018, p. 15).

Some scholars have expressed more critical positions with respect to the modernization of the data protection system brought about by the GDPR, which has been considered a "downgrade" in terms of personal protection because it would not adequately defend the individual rights of the person at the public level and would neglect the side of collective protection (Piraino, 2017, p. 405). Others considered the content of the new personal data protection legislation "disappointing", especially regarding the balance achieved between fundamental rights and market needs (Thiene, 2017).

(a) Scope of the GDPR and main principles of data processing

The delimitation of the scope of application of the GDPR is to be counted among the novelties of this discipline which establishes a significant extension concerning that offered by the former one (Directive 95/46/EC). In this context, the EU legislator demonstrates that it has implemented the most recent guidelines of the Court of Justice[3]. As a result of the Art. 3, the GDPR applies to any activity carried out by a data controller or a data processor in the Union, regardless of whether or not the processing is carried out in the Union. When certain conditions are met, however, the GDPR also applies to the processing carried out by the owner or manager who is not established within the Union, which implies the applicability of the European regulation also to those treatments carried out outside the EU. European Union, provided that the services connected to such treatments are offered to data subjects located within it.

As regards the material scope of application of the GDPR, it includes the entirely or partially automated processing of personal data as well as the non-automated processing of personal data contained in a file or intended to be included therein (Art. 1). The GDPR also establishes the principles applicable to the data processing activities (art. 5), namely: lawfulness, correctness and transparency purpose limitation, so that the data is collected for

[3] See in particular the judgments *Google Spain SL*, *Schrems* and *Digital Rights Ireland Ltd*.

delimited, explicit and legitimate purposes; minimization of data, so that only the information necessary to fulfill the intended purposes is collected; accuracy of the data and limitation of their conservation for a time not exceeding that necessary; and finally, data integrity and confidentiality. Within these principles, particular importance is assumed by lawfulness, which exists only where the interested party has given his consent to the processing, or the same appears necessary to achieve one of the strictly established purposes (art. 6).

More stringent requirements apply to the "particular categories of data" (formerly sensitive data), which, under the GDPR, include not only any data suitable for revealing information such as racial or ethnic origin, political opinions, religious or philosophical beliefs, and union, but also genetic data, biometric data, and data relating to the health or sex life and sexual orientation of the individuals concerned (Art. 9). The general rule that prohibits the processing of such data is followed by a series of potentially very wide-ranging exceptions. Firstly, these categories of data can be processed whenever there is explicit consent, or where the data have been manifestly made public by the data subject himself (Art. 9). Furthermore, the processing of such data is permitted where this is necessary for the pursuit of more specific purposes, which fall within the notion of "public interest". The scope of discretion exercisable by the Member States, therefore, depends on the breadth of this notion, which can be widened or narrowed according to purposes deemed worthy to being pursued.

In summary, considering the discipline offered by the GDPR, it is possible to state that the processing of personal data must be lawful and limited to the specific purposes assumed by the processing itself. The data collected must be accurate and the forms of archiving must be such to facilitate their treatment, cancellation, and rectification without delay. Furthermore, the same must be kept for the time necessary to achieve the purposes for which they were collected. The data must be treated in such a way that they are protected from any unauthorized or illicit use, and must be safeguarded with adequate technical and organizational measures to prevent them from being lost, destroyed or accidentally damaged.

Enhancing data protection and cybersecurity

As previously underlined, the adoption of a potentially all-encompassing definition of personal data seems to be accompanied by an – albeit not manifest – an acknowledgment of the difficulties of guaranteeing complete anonymization of data in the digital age. This is matched by a new vision of the data protection system itself, inspired by the principles of precaution and risk prevention for the rights and freedoms of the persons concerned. Within the Regulation, this vision takes the form of accountability – a duty to give an account – attributed to the data controller, in particular by Art. 32, which assumes the aim of stimulating the adoption of "proactive behaviours and measures suitable" for demonstrating and ensuring the correct application of the EU legislation, from a perspective of preventive protection (Colapietro, 2018, p. 27).

The latter certainly include the principles of "privacy by design" and "privacy by default" (Art. 25, GDPR), but also the preventive impact assessment, to be carried out in the case of

treatment of some categories of data, including those collected and/or processed through "new technologies". Beyond this specific hypothesis, the GDPR assigns the data controller the task of carrying out this assessment in consideration of the nature of the data collected, their object, the context, and the purposes of the processing (Art. 35). Within the discretion recognized to the data controller, the GDPR states that, in any case, this evaluation must be carried out in the case of systematic and extensive "evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person" (Art. 35). Furthermore, the impact assessment is also explicitly required in the case of large-scale processing of sensitive data and data relating to crimes and/or criminal convictions, and in the case of "large-scale systematic surveillance of an area accessible to the public" (Art. 36). In this context, the GDPR prescribes the adoption of pseudonymization and encryption procedures for the data in question, which correspond to the same number of certificates of authenticity and mechanisms for authenticating the subjects authorized to access. Furthermore, it appears worthy of note that the GDPR suggests the adoption of initiatives aimed at training and raising the awareness of the personnel involved in the processing activities (art. 39), possibly also through the definition of specific codes of conduct which assume the aim to contribute to the correct application of the Regulation (art. 40).

For this work, it should be highlighted how the proliferation of forms of personal data collection on the most disparate personal and social spheres places us before an even greater risk than the "mere" violation of privacy, i.e., that of abusive reuse of data, better known as "data misuse". The misuse of data is particularly relevant when considering dematerialized data and alludes to the possibility that the data collected in a certain area and for certain purposes are used in further areas and for the pursuit of completely different ones – think of the case of genetic profiling, which has become a "case study" due to the proliferation of genetic screening services for prevention purposes. The accumulation of such information by private companies – together with the relative reuse rights, usually transferred by the user himself at the very moment of signing the contract – leads to the creation of huge databases which could be consulted – legitimately or not – for stealing information that can be used in fields unrelated to that of healthcare. Further examples of data misuse include the reuse of genetic information for personnel selection purposes, or to determine risk percentages in the context of stipulating a health insurance contract, which has been appropriately renamed as "genetic discrimination" (Faralli, 2020).

The strategic role assumed by health data is confirmed by the fact that the EU Directive 2022/2555, relating to measures for a high common level of cybersecurity in the Union (also known as "NIS 2") has included the health sector among those "highly critical". Moreover, after having overcome the distinction between digital service providers and operators of essential services of the previous EU Directive 2016/1148 f – considered obsolete due to the complexity of current protection needs –, has expressly included both the health service and the digital service providers in the category of subjects who must comply with the more

stringent and detailed measures regarding the management of cybersecurity risks and the related reporting obligations (Art. 21).

Pervasive technologies and privacy concerns: the case of contact tracing

Insofar as the ICTs become increasingly pervasive, colonizing an increasing number of portions of our social life, health and personal data collected for a given purpose may be susceptible to legitimate reuse, based on the conditions dictated by GDPR itself. This is what happened due to the outbreak of the COVID-19 pandemic, the spread of which on a global scale has threatened the health of a large part of the world's population and drastically affected fundamental freedoms and individual rights. From the beginning of the pandemic to today, numerous examples have been reported of the use of new technologies aimed at containing the contagion, and in particular at controlling compliance with the provisions adopted during the emergency decree to protect the population. In the European context, the debate relating to the use of the latter has been largely monopolized by the development and adoption of apps for "proximity tracking" – more commonly known as contact tracing –, the spread of which has represented a large test for the overall tightness of the system set up by the GDPR a few years after it entered into force. It is worth clarifying that the level of exposure of individual privacy in the use of these services appeared to be closely related to the technical configurations adopted by the service providers, as well as to the broader regulatory context within which they were intended to operate. With regard to the EU framework, there is no doubt that subject to compliance with the general principles applicable to the processing of personal data, the GDPR allows for the collection and processing of personal data relating to health by public authorities, regardless of the data subject's consent, when this is necessary, among other things, to deal with "serious cross-border threats to health" (Art. 9, GDPR) which was that represented by the dissemination of the COVID-19 on a global scale.

The progressive adoption of these services by the EU countries has been carefully monitored by the European Data Protection Board (EDPB), which has released a series of documents aimed at ensuring that this form of innovation complies with the system set up by the GDPR, as well as the fundamental principles of the functioning of the EU and, in particular, those set out in the EU Charter of Fundamental Rights. More specifically, the EDPB had the opportunity to underline how the development of contact tracing applications should have followed "accountability criteria", to be pursued through the documentation relating to the impact assessment conducted for data protection, as well as through the implementation of mechanisms inspired on the principles of the privacy by design and privacy by default (European Data Protection Board, 2020a). Furthermore, the EDPB stressed that the source code should be made public to allow for the widest possible evaluation by the scientific community. The EDPB has done its utmost to recommend that the adoption of contact tracing applications take place on a voluntary basis, considering this choice more in line with the fundamental values of the EU legal framework, but also as a "token" of responsibility by the

population (European Data Protection Board, 2020a). At the same time, the EDPB also expressed its opinion on the use of location data of users' mobile devices collected by telecommunications service providers. More in detail, the EDBP underlined that the ePrivacy Directive (Dir. 2020/58/EC) allowed the introduction of exceptional legislative measures aimed at safeguarding public security (European Data Protection Board, 2020b). Nonetheless, the EDPB itself remarked that such measures could be considered legitimate only if they appeared necessary, adequate, and proportionate to the aims pursued and in any case in line with the respect for democratic values. In particular, recalled the EDPB, these measures had to comply with the EU Charter of Fundamental Rights and with the European Convention for the Protection of Human Rights and Fundamental Freedoms while still remaining subject to the judicial review of the Court of Justice of the Union and of the European Court of Human Rights (European Data Protection Board, 2020b). Within the EDPB, however, there seems to have been a change of orientation with respect to this possibility, as evidenced by the Letter sent to the European Commission on 14 April 2020, which argued that the functioning of contact tracing applications was independent from the location of users' mobile devices and that their primary objective was not to follow "the movements of individuals or to enforce prescriptions. The main function of such apps is to discover events (contacts with positive persons), which are only likely and for the majority of users may not even happen" (European Data Protection Board, 2020a, p. 2). Moreover, the EDPB clarified that collecting data about the individuals' movements in the context of contact tracing apps "would violate the principle of data minimisation" as well as "create major security and privacy risks" (European Data Protection Board, 2020a, p. 2).

Conclusions

As highlighted within this work, the enactment of the GDPR has sealed the indissoluble connection between the protection of personal data and their "free" circulation in the EU area. The importance of this connection is demonstrated by the new proposal for a Regulation on the European Health Data Space (cited above) which is meant to stimulate the development of new products and services data-driven in the healthcare domain. The pursuit of a common health data space is linked to the goal of exploiting the socio-economic advantages offered by their use and must be read in conjunction with the issue of EU Regulation No. 1807/2018 on the free circulation of non-personal data in the EU. In this context, the latter Regulation sets itself an ambitious goal, namely the introduction of a "fifth freedom" of movement that adds to those relating to goods, services, capital, and people, which represent a fundamental pillar in the entire EU integration process. To allow the pursuit of this objective, Regulation No. 1807/2018 has imposed the elimination of localization obligations unless they are justified by reasons of public safety in compliance with the principle of proportionality (art. 4). In this way, the aim is to create a single European market for archiving (hosting) services and other data processing services, thus exploiting the enormous growth opportunities related to the data economy.

Although the protection of personal data and the free movement of non-personal data appear clearly distinguishable – at least on paper –, the interferences between one and the other can be multiple. It is worth recalling that the category of non-personal data includes information that is impersonal by nature, i.e., *ab initio*, and which therefore does not allow identification of the subjects from whom it was collected, as well as personal information that has been subjected to a process of anonymization or depersonalization at a time following that of their collection. Due to their intrinsic nature, however, it is possible to state that the processing of health data allows in most cases the identifiability of the interested party, which leads us to believe that the free circulation of health data mostly concerns personal information submitted to the anonymization process. In this latter regard, however, it should be remembered that, in the light of the unreliability of personal data anonymization processes (mentioned above, paragraph 4), the possibilities of reverse engineering anonymized data remain considerable, which exposes the information contained therein to a very concrete vulnerability.

As we have seen in this work, the EU has embraced a vision within which data are considered the driving force of economic development in the coming decades, as well as a key factor in being able to stand the economic and geopolitical comparison with the other global powers. In this context, therefore, it seems possible to state that the idea of personal data protection is severely tested by the emergence of multiple drives aimed at collecting, storing, processing and reusing health data (and not only), which correlate numerous possibilities of economic exploitation, all in a context of growing penetration of new technologies within today's health systems. However, as adequately emphasized in the Code of Ethics adopted by the International Medical Informatics Association (2016), health data “not only reveal much that is private and that should be kept confidential but, more importantly, function as the basis of decisions that have profound welfare implications for their subjects”. This type of concern is reflected in the findings offered by the legal doctrine in this sector, which highlights how the processes of technological innovation linked to the expansion of the ICTs have triggered the “widespread feeling” that our data is constantly at risk (Colapietro, 2018, p. 2). In this perspective, it is possible to argue that a main challenge for the protection of health data is their intrinsic vulnerability, a connotation that derives directly from their attractiveness, especially for those subjects – mostly commercial companies – who are able to process, reuse and profit from them.

References

BASSINI, M. 2016. La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali. *Quaderni Costituzionali*, **3**:587-589.

BOTRUGNO, C. 2018. *Telemedicina e trasformazione dei sistemi sanitari. Un’indagine di bioetica*. Roma, Aracne.

_____. 2021. Information technologies in healthcare: enhancing or dehumanising doctor-patient interaction? *Health*, **25**(4):475-493.

COLAPIETRO, C. 2018. I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale. *Federalismi.it*, **22**:1-34.

COMANDÉ, G. 2019. Ricerca in sanità e data protection: un puzzle... risolvibile. *Rivista Italiana di Medicina Legale*, **1**:187-208.

DUCATO, R. 2016. La crisi della definizione di dato personale nell'era web 3.0. *In*: F. Cortese; M. Tomasi (orgs.), *Le definizioni nel diritto*. Napoli, Quaderni della Facoltà di Giurisprudenza, pp. 145-178.

EUROPEAN COMMISSION. 2004. *e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004DC0356&from=EN.

_____. 2018. *Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society.* Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC023 3&from=EN.

_____. 2020. *Communication on a European Strategy for Data*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN.

EUROPEAN DATA PROTECTION BOARD. 2020a. *Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic*. Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

_____. 2020b. *Statement on the processing of personal data in the context of the COVID-19 outbreak*. Available at: https://edpb.europa.eu/sites/default/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

FARALLI, C. 2020. Genetic data and discrimination. *Jura Gentium*, **17**(1):179-186.

FINOCCHIARO, G. 2017. Introduzione al regolamento europeo sulla protezione dei dati personali. *Nuove Leggi civili commentate*, **1**:1-18.

_____. 2018. Riflessioni sul poliedrico Regolamento europeo sulla privacy. *Quaderni Costituzionali*, **4**:895-897.

INTERNATIONAL MEDICAL INFORMATICS ASSOCIATION. 2016. *Code of Ethics for Health Information Professionals*. Available at: https://imia-medinfo.org/wp/imia-code-of-ethics/.

LIU, V., MUSEN, A., CHOU, T. 2015. Data Breaches of Protected Health Information in the United States. *Journal of American Medical Association*, **313**(14):1471-1473.

LUPTON, D. 2013. The digitally engaged patient: self-monitoring and selfcare in the digital era. *Social Theory and Health*, **11**(3):256-270.

PEDRAZZI, G. 2019. Il ruolo del responsabile della protezione dei dati (DPO) nel settore sanitario. *Rivista Italiana di Medicina Legale*, **1**:179-186.

PIRAINO, F. 2017. Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato. *Nuove Leggi Civili Commentate*, **40**(2):369-409.

PURTOVA, N. 2018. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, **10**:1-35.

THIENE, A. 2017. Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo Regolamento europeo. *Nuove Leggi Civili Commentate*, **2**:410-444.

VERIZON. 2018. *Data Breach Investigation Report*. Available at: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pd

WORLD HEALTH ORGANIZATION. 2010. *Report on the second global survey on e-health*. Available at: www.who.int/goe/publications/goe_telemedicine_2010.pdf

Submetido: 26/03/2023
Aceito: 09/05/2023