GOVERNANCE AND PROCESSING OF PERSONAL DATA IN THE ITALIAN HEALTHCARE SYSTEM IN THE LIGHT OF EU PRINCIPLES

GOBERNANZA Y TRATAMIENTO DE DATOS PERSONALES EN EL SISTEMA SANITARIO ITALIANO A LA LUZ DE LOS PRINCIPIOS DE LA UE

Actualidad Jurídica Iberoamericana Nº 20, febrero 2024, ISSN: 2386-4567, pp. 1052-1087

Francesco
GIACOMO
VITERBO

ARTÍCULO RECIBIDO: 20 de noviembre de 2023
ARTÍCULO APROBADO: 12 de enero de 2024

RESUMEN: The study focuses on the new model of governance of personal data in the healthcare system, which is going to be implemented in Italy and in the Union on the basis of the principles of findability, accessibility, interoperability and reusability of data (FAIR principles), set out in 2020 by the 'European strategy for data' and taken as a reference by the subsequent Data Governance Act. The problematic issues relating to the primary and secondary use of electronic health data call for a special effort, especially on the part of the supervisory authorities, in preserving compliance with the GDPR principles in this renewed context. The most important challenge is to ensure that EU fundamental rights remain the central element in the digital transformation through a human-centric approach to the new issues prompted by societal demands for data sharing and availability.

PALABRAS CLAVE: Digital transformation; e-health data; primary use; secondary use; accessibility; availability; reusability; data sharing; data altruism.

ABSTRACT: *El estudio se centra en el nuevo modelo de gobernanza de los datos personales en el sistema sanitario, que se va a implantar en Italia y en la Unión sobre la base de los principios de disponibilidad, accesibilidad, interoperabilidad y reutilización de los datos (principios FAIR), establecidos en 2020 por la "Estrategia europea para los datos" y tomados como referencia por la posterior Ley de Gobernanza de Datos. Las cuestiones problemáticas relacionadas con el uso primario y secundario de los datos sanitarios electrónicos exigen un esfuerzo especial, sobre todo por parte de las autoridades de supervisión, para preservar el cumplimiento de los principios del RGPD en este contexto renovado. El reto más importante es garantizar que los derechos fundamentales de la UE sigan siendo el elemento central de la transformación digital a través de un enfoque centrado en el ser humano de las nuevas cuestiones suscitadas por las demandas sociales de intercambio y disponibilidad de datos.*

KEY WORDS: *Transformación digital; datos electrónicos de salud; uso primario; uso secundario; accesibilidad; disponibilidad; reutilización; uso compartido de datos; altruismo de datos.*

SUMARIO.- I. DISTINCT CULTURAL APPROACHES TO THE ISSUE OF PERSONAL DATA PROTECTION IN THE CONTEXT OF NEW CHALLENGES POSED BY DIGITAL TRANSFORMATION.- II. PROCESSING OF PERSONAL DATA IN THE ITALIAN HEALTHCARE SYSTEM AND THE PRINCIPLE OF LAWFULLNESS: DOWNSIZING THE ROLE OF CONSENT.- III. SAFEGUARDS FOR THE PROCESSING OF HEALTH AND GENETIC DATA AND THE PRINCIPLE OF ACCOUNTABILITY.- IV. RECENT EVOLUTION OF DOMESTIC AND EUROPEAN LAW IN FAVOR OF SHARING AND REUSE OF HEALTH DATA: PREMISES FOR A POLICY OF DATA INTEGRATION AND INTEROPERABILITY.- V. THE 'EUROPEAN STRATEGY FOR DATA', THE F.A.I.R. PRINCIPLES AND THE SECONDARY USE OF HEALTH DATA FOR SCIENTIFIC RESEARCH PURPOSES.– VI. THE 'ALTRUISM OF DATA' AND THE GOAL OF CREATING A EUROPEAN COMMON HEALTH DATA SPACE.– VII. PROBLEMS AND NEW CHALLENGES OF THE RECENT EUROPEAN APPROACH TO DATA GOVERNANCE IN HEALTHCARE.

I. DISTINCT CULTURAL APPROACHES TO THE ISSUE OF PERSONAL DATA PROTECTION IN THE CONTEXT OF NEW CHALLENGES POSED BY DIGITAL TRANSFORMATION.

What are "personal data"? What legal nature do they have? To whom does personal data belong? Can they be commercialized? How can or should they circulate in new and complex environments such as the Infosphere or the so-called *Digital Single Market*?[1]

1 A definition of 'personal data' has been provided by both the (repealed) Directive 95/46/EC under Article 2(a) and the current Regulation (EU) 2016/679 (*General Data Protection Regulation* - GDPR) under Article 4(1): 'any information relating to an identified or identifiable natural person ('data subject')', in the meaning specified therein. This notion, however, and the data protection rules themselves have left open numerous questions regarding, in particular, their legal nature, their commercial value, as well asthe possibility of delineating them in proprietary terms: on these problematic profiles, reference may be made to Viterbo, F.G.: *Protezione dei dati personali e autonomia negoziale*, Naples, 2008; Id.: "Freedom of contract and the commercial value of personal data", *Contratto e impresa/Europa*, 2-2016, p. 593 ff.; Id.: "The 'User-Centric' and 'Tailor-Made' Approach of the GDPR Through the Principles It Lays down", *Italian Law Journal*, 2-2019, p. 631 ff. In recent years,the debate on these issues has expanded considerably and has been enriched by numerous contributions from the doctrine, partly as a result of the most recent regulatory measures adopted - or in the process of final adoption - by the Union under the *Digital Single MarketStrategy for Europe* launched in 2015 and the *European Strategy for data* adopted in 2020: see Communication from the Commission, *Strategy for a Digital Single Market in Europe*, May 6,2015, COM(2015) 192 final, available at *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192*; Communication from the Commission, *European Strategy for data*, February 19, 2020, COM(2020) 66 final, available at *https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066*. In the Italian literature, see Perlingieri, P.: "Privacy digitale e protezione dei dati personali tra persona e mercato", *Foro nap.*, 2-2018, p. 481 ff.; Id.: "Sul trattamento algoritmico dei dati", *Tecn. Dir.*, 2020, p. 181 ff.; Stanzione, P.: "Introduzione", in Id. (ed.): *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Turin, 2022, p. 1 ff.; Sica, S. and D'Antonio, V.: "La commodification dei dati personali nella data driven society", *ibid*., p. 129 ff.; Pizzetti, F.: "GDPR, Codice novellato e Garante nell'epoca dei Big Data e dell'Intelligenza Artificiale", in Id. (ed.), *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, Turin, 2021, p. 234 ff.; Ricciuto, V.: "Circolazione e scambio dei dati personali. Il problema della regolazione del nuovo fenomeno patrimoniale", *Riv. dir. impr.*, 2021, p. 261 ff.; Id.: "La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno", in Id., Cuffaro V., D'Orazio R. (eds.), *I dati personali nel diritto europeo*, Torino, 2019, p. 23 ff.; De Franceschi, A.: "Il «pagamento» mediante dati personali", *ibid*., p. 1381 ff.; Camardi, C.: "Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali", *Giust. civ.*, 2019, p. 499 ff.; Thobani, S.: "Il pagamento mediante dati personali", in S. Orlando, G. Capaldo (eds.), *Annuario 2021 Osservatorio*

• Francesco Giacomo Viterbo
Associate Professor of Private Law at the University of Salento, Italy. E-mail: francesco.viterbo@unisalento.it

These are some crucial underlying questions and issues that scholars and scientists (jurists, economists, sociologists, marketing experts, medical doctors, and now data scientists) have long been trying to answer, fascinated by the new challenges posed by the digital transformation in its many declinations: Internet of Things, *Blockchain*, Big Data, Artificial Intelligence, Robotics, Telemedicine, etc.

At least three different cultural approaches to the topic of legal regulation of personal data protection confront each other in the global landscape in the current digital age[2], providing different answers to the aforementioned questions:

a) state-centric approach

b) market-centric approach

c) human-centric approach.

The state-centric approach is implemented when the state government has systematic access to the mass of personal information managed by the private sector and uses advanced technological means, collecting and processing personal data on a mass scale in order to profile all citizens and shape public policies. In this view, personal data are treated as public goods, as they belong to the government, which is able to process them for purposes of social utility (e.g., citizen safety) or social control (including crime prevention)[3]. A concrete example of this approach may be China's Social Credit System, a system for assessing the social reputation of individuals, companies and local governments, developed by the Chinese government to monitor the trustworthiness of its 1.3 billion citizens based on real profiling related to negative (e.g., unpaid debts, fines, reports, etc.) and positive (e.g., social services, volunteering, on-time payments, etc.)[4]. This system uses the

Giuridico sulla Innovazione Digitale, Roma, 2021, p. 361 ff.; Versaci, G.: "Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection", *Eur. Rev. C. L.*, 2018, p. 374 ff.; Spatuzzi, A.: "Contratto di fornitura di servizi digitali e ruolo del consenso al trattamento dei dati personali", *Notariato*, 2021, p. 371 ff.; and also see the following monographic works: Ricciuto, V.: *L'equivoco della privacy. Persona vs. dato personale*, Naples, 2022; Irti, C.: *Consenso "negoziato" e circolazione dei dati personali*, Turin, 2021; Floridi, L.: *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milan, 2017, p. 27 ff.

2 On this topic see Calzada, I.: "Citizens' Data Privacy in China: The State-of-the-Art of the Personal Information Protection Law (PIPL)", *Smart Cities*, 2022, 5, p. 1129 ff., who compare the 'three main worldwide data privacy paradigms that exist at present: (i) the General Data Protection Regulation (GDPR) in the E.U., (ii) the California Consumer Privacy Act (CCPA) in the U.S., and (iii) the Personal Information Protection Law PIPL', recently adopted in China.

3 In this regard see Cate, F.H. Dempsey, J.X. and Rubinstein, I.S.: "Systematic government access to private-sector data", *International Data Privacy Law*, 2012, p. 195 ff.

4 The project was initiated with the *Planning Outline for the Construction of a Social Credit System (2014-2020)*. This document mentions the aim to promote 'integrity in government affairs', 'commercial sincerity', 'social integrity' and 'judicial public trust' which shows that these measures are targeted at individuals, as well as companies, judicial organs, and other governmental authorities. In February 2018, one such programme was implemented in Shanghai through the 'Honest Shanghai' app, which uses facial recognition software linked to government records. In January 2019, the Beijing government officially announced the introduction of the 'Personal Credit Score', based on penalty and award mechanism. For more details,

technology of *Big data* analysis and can be considered a form of mass surveillance[5]. It is, however, clear that such an approach poses a number of threats to equality, personal freedom and democracy [6].

The market-centric approach considers the asset value of personal data as a tool for market development. L'essenza di questo approccio consiste nell'autorizzare di *default* le entità private affamate di dati o nel consentire il commercio e la vendita di dati personali, *de jure* o *de facto*, al fine di promuovere la libera circolazione delle informazioni sul mercato. Moreover, personal data, having commercial value, would be equated with appropriable commodities[7]. Commodification of information would be inevitable, especially for consumers with regard to their personal data[8]. Moreover, it is emphasized that this process would lead to a higher level of protection, taking property rights (industrial and intellectual) as a reference. This means that, if personal data are considered similar to a commodity that can be intended for appropriation or commercial exploitation, the regime of copyright protection and contract law might apply[9].

In contrast, the European approach to online privacy and data protection issues seems to differ from the aforesaid approaches. Considering both Directive

see Liang, F. Das, V. Kostyuk, N. Hussain, M.: "Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure", *Policy & Internet*, 2018, p. 415 ff.; Kostka, G.: "China's social credit systems and public opinion: Explaining high levels of approval", *New Media & Society*, 2019, p. 1565 ff.; Mac Síthigh, D. Siems, M.: "The Chinese social credit system: a model for other countries?", *Modern Law Review*, 2019, p. 1034 ff.

5 Some recent studies have shown that punitive or afflictive consequences for a negative credit score affect a very limited number of people and that the system, as a whole, is characterised by excessive fragmentation: v. Drinhausen, K. Brussee, V.: "China's Social Credit System in 2021: From fragmentation towards integration", 2021, available at *https://merics.org/en/report/chinas-social-credit-system-2021-fragmentation-towards-integration*.

6 In this regard, it is curious to note that initiatives based on scoring reward mechanisms associated with 'virtuous' citizen behaviour in various sectors (environment, taxation, culture, mobility, sport) have also been taken in Italy. The Italian Data Protecion Authority (Garante per la protezione dei dati personali) has recently launched three preliminary investigations concerning a series of projects promoted by public and private entities, which envisage the assignment of scores also with respect to data collections provided voluntarily by the data subjects. As stated in the communication of 8 June 2022 (web doc. no. 9778361), the interventions of the Authority were necessary because of the risks connected to profiling mechanisms involving a sort of 'citizenship by points', from which negative legal consequences on the rights and freedoms of the data subjects could derive.

7 On this point see Nissenbaum, H.: "A Contextual Approach to Privacy Online", *Daedalus*, 2011, p. 140 ff.

8 Bartow, A.: "Our Data, Ourselves: Privacy, Propertization, and Gender", *University of San Francisco Law Review*, 2000, p. 634 ff.

9 This approach has been proposed in particular by US scholars: Posner, R.A.: "The Right of Privacy", *Georgia Law Review*, 1977, p. 393 ff.; Litman, J.: "Information Privacy/Information Property", *Stanford Law Review*, 2000, p. 1283 ff.; Zittrain, J.: "What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication", *Stanford Law Rev.*, 2000, p. 1201 ff.; Lessig, L.: "Privacy as Property", *Social Research*, 2002, p. 247 ff.; Schwartz, P.M.: "Property, Privacy and Personal Data", *Harvard Law Review*, 2004, p. 2056 ff., available at *http://scholarship.law.berkeley.edu/facpubs/2150*; in the Italian literature, see Ubertazzi, L.C.: "Banche dati e privacy", *Diritto industriale*, 2002, p. 633 ff.; Zeno Zencovich, V.: "Profili negoziali degli attributi della personalità", *Dir. inf.*, 1993, p. 547 ff. In the European literature, see Poullet, Y.: "Data Protection Between Property and Liberties. A Civil Law Approach", in H.W.K. Kaspersen, A. Oskamp eds, *Amongst Friends in Computers and Law. A Collection of Essays in Remembrance of Guy Vandenberghe*, The Hague, 1990, p. 160 ff.; Bygrave, L.A.: *Data Protection Law. Approaching its Rationale, Logic and Limits*, L'Aia, 2002, p. 120 ff.; Purtova, N.: *Property Rights in Personal Data: a European perspective*, L'Aia, 2011.

95/46 and Regulation (EU) 2016/679 (hereafter: GDPR), the legal system of the European Union seems to have embraced a human-centric approach inspired by the values of personalism and human dignity[10]. This human-centric approach can be deduced from the European data protection framework, where there is no room for a specific contract that allows the data subject or the data controller to dispose of personal data. Moreover, recital 24 of 'Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services' recognizes that 'the protection of personal data is a fundamental right and therefore personal data cannot be considered as a commodity'[11]. There is no room for the commodification of personal data in both the wording and logic of Articles 7 and 8 of the EU Charter of Fundamental Rights likewise.

The latter approach is built around two very broad notions, that of "personal data" and that of "processing" defined in nn. 1) and 2) of Article 4 GDPR, and is based on the the "principles relating to processing of personal data" set forth in Article 5. The GDPR, with a view to the accountability principle, imposes on the data controller a prior case-by-case assessment of the lawfulness, fairness and transparency of the data processing, which also requires compliance with the principles of purpose limitation, data minimisation, storage limitation, accuracy, integrity and confidentiality[12].

This assessment always requires an adequate factual answer to the following preliminary questions:

10 See Recital 4 of the GDPR, which specifies that '[t]he processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality'. Approaching these issues in the light of the fundamental principles laid down in the EU Treaties and the Constitutions of the EU Member States is of great importance: Perlingieri, P.: "Privacy digitale e protezione dei dati personali tra persona e mercato", cit., p. 481 ff.; Gambino, A.: "Dignità umana e mercato digitale", in G. Contaldi (ed.), *Il mercato unico digitale*, Rome, 2017, p. 7 ff.

11 The 'Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services' is available at *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770*. Recital 24 specifies that the Directive applies 'to contracts where the trader supplies, or undertakes to supply, digital content or a digital service to the consumer, and the consumer provides, or undertakes to provide, personal data', ensuring 'that consumers are, in the context of such business models, entitled to contractual remedies'. It is important to note that, compared to the initial draft of this directive [COM(2015)0634 - C8-0394/2015 - 2015/0287(COD)], the final text has removed references to the provision of personal data as 'consideration': on this point see European Data Protection Supervisor (EDPS), "Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content", adopted on 14 March 2017, available at *https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf*). See also Clifford, D. Graef, I. Valcke, P.: "Pre-formulated Declarations of Data Subject Consent - Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections", *German Law Journal*, 2019, p. 679 ff.; Finocchiaro, G.: "Il quadro di insieme sul Regolamento europeo sulla protezione dei dati personali", in Ead. (ed.), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, p. 2 ff.

12 On the meaning and importance of the Article 5 GDPR principles, with particular regard to the accountability principle, see Viterbo, F.G.: "The 'User-Centric' and 'Tailor-Made' Approach of the GDPR", cit., p. 659 ff. More generally, on the distinction between principles and rules and their relationship, see Perlingieri, P. and Femia, P.: *Nozioni introduttive e principi fondamentali del diritto civile*, Napoli, 2000, p. 13 ff.; Federico, A.: "Applicazione dei princípi generali e funzione nomofilattica", *Rass. dir. civ.*, 2018, p. 820 ff.; Femia, P.: "Tre livelli di (in)distinzione tra princípi e clausole generali", in G. Perlingieri, M. D'Ambrosio (ed.), *Fonti, metodo e interpretazione*, Napoli, 2017, p. 209 ff.

a) Is there a legitimate basis for processing personal data?

b) What purpose(s) does the processing of personal data serve? Is the processing compatible with the purposes for which the personal datawere initially collected?

c) Is the data processed adequate, relevant, and limited to what is necessary?

d) Is the data processed accurate? Do they need to be updated?

e) How long can they be stored?

f) What technical and organisational security measures can be taken from the design of the data processing and by default to prevent data alteration, unauthorised access or other breaches that could harm or jeopardise data subjects' rights?

g) Who has the responsibility and duty to prove compliance with data protection principles and rules?

II. PROCESSING OF PERSONAL DATA IN THE ITALIAN HEALTHCARE SYSTEM AND THE PRINCIPLE OF LAWFULLNESS: DOWNSIZING THE ROLE OF CONSENT.

Having said that, we intend to analyse here how this framework of principles and rules in force in Italy and Europe holds up with regard to the processing of personal data in the healthcare system[13] and in the light of the recent 'European Strategy for Data' [14].

13 On this topic see Perlingieri, C.: "eHealth and Data", in R. Senigaglia, C. Irti, A. Bernes (eds.), *Privacy and Data Protection in Software Services*, Springer ed., 2021, p. 127 ff.; Ead.: "Coronavirus e tracciamento tecnologico: alcune riflessioni sull'applicazione e sui relativi sistemi di interoperabilità dei dispositivi", *Actual. iur. iberoam.*, 2020, p. 836 ff.; Pizzetti, F.: "La Parte I del Codice novellato", in Id. (ed.), *Protezione dei dati personali in Italia*, cit., p. 114 ff.; Ferola, L.: "Le 'misure di garanzia' a tutela dei dati biometrici, genetici e sulla salute", *ibid.*, p. 411 ff.; Guarda, P.: "I dati sanitari", in V. Cuffaro, R. D'Orazio, V. Ricciuto (eds.), *o.c.*, p. 591 ff.; Ciancimino, M.: *Protezione e controllo dei dati in ambito sanitario e intelligenza artificiale*, Naples, 2020. Cfr. Becker, R., Comandé, G. et Al.: "Secondary Use of Personal Health Data: When Is It "Further Processing" Under the GDPR, and What Are the Implications for Data Controllers?", *Eur. J. Health Law*, 2022, p. 1 ff.; Orviský, M., Klátik, J.: "Telemedicine as a part of globalization and tool for innovation from the legal point of view", *SHS Web of Conf.*, 92, 2021, p. 6 ff.; Marelli, L., Lievevrouw, E., Van Hoyweghen I.: Fit for purpose? The GDPR and the governance of European digital health", *Policy Studies*, 2020, p. 447 ff.; Amram, D.: "Building up the "Accountable Ulysses" model. The impact of GDPR and national implementations, ethics, and health-data research: Comparative remarks", *Computer Law & Security Review*, 37, 2020, p. 1 ff. With reference to the legislation prior to the reform carried out by Legislative Decree No 101 of 10 August 2018 (and, therefore, to the entry into force of the GDPR), see Finocchiaro, G.: "Il trattamento dei dati sanitari: alcune riflessioni critiche a dieci anni dall'entrata in vigore del Codice in materia di protezione dei dati personali", in G.F. Ferrari (ed.), *La legge sulla privacy dieci anni dopo*, Milan, 2008, p. 207 ff.; Caggia F.: "Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario", in V. Cuffaro, R. D'Orazio, V. Ricciuto (eds.), *Il codice del trattamento di dati personali*, Turin, 2007, p. 405 ff.; Maschio F.: "Il trattamento dei dati sanitari. Regole generali e particolari del trattamento per finalità di rilevante interesse pubblico", in G. Santaniello (ed.), *La protezione dei dati personali*, in Id. (dir.), *Trattato di diritto amministrativo*, XXXVI, Padova, 2005, p. 485 ff.; Di Ciommo, F.: "La privacy sanitaria", in R. Pardlesi (ed.), *Diritto alla riservatezza e circolazione dei dati personali*, Milan, 2003, p. 239 ff.; Ciatti, A.: "La protezione dei dati idonei a rivelare lo stato di salute nella legge n. 675 del '96", *Contr. impr./Eur.*, 1998, p. 368 ff.

14 On the European Data Strategy, see Cerrina Feroni, G.: "Luci e ombre della Data Strategy europea", 13 maggio 2022, in *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9769786*; Bravo, F.:

Among the data that are processed in healthcare system, there are some special categories of personal data under Article 9 GDPR, namely data concerning health (defined by No. 15 of Article 4 GDPR) and genetic data (defined by No. 13 of the same Article).[15].

Here, the human-centric approach of the GDPR is seriously challenged, since health data externalise the most vulnerable and delicate aspects of the person, but at the same time, they can acquire both a high commercial value in the market, and an extremely relevant social value: think of the importance they can have for private individuals investing in the pharmaceutical industry or producing or marketing specific products for people suffering from particular pathologies (e.g. celiac disease); at the same time, think of their centrality for medical scientific research or for Artificial Intelligence research through their algorithmic processing, and also for public health policy management.

A first observation arising from the analysis of the multilevel regulation (EU regulation, national legislation, measures of the Italian Data Protection Authority, henceforth: Garante) of the health data processing concerns the way the lawfulness principle operates. Beyond the general prohibition to process the 'special categories

"Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act", *Contr. impr./Eur.*, 2021, p. 199 ff. On recent European policies on health and new technologies, see Irti, C.: "L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano", *Persona e mercato*, 2023, p. 32 ff.

15 Article 4(1)(15) defines 'data concerning health' as those 'personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status'. Recital 35 specifies that this definition covers 'all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject'; it includes 'information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test'. per una breve analisi di tali aspetti definitori, v. Bygrave, L.A., Tosoni, L.: "Article 4(15). Data concerning health", in C. Kuner, L.A. Bygrave, C. Docksey, (eds), *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford, 2020, p. 217 ff.; cfr. Guarda, P.: "I dati sanitari", cit., p. 593 ff. In giurisprudenza, cfr. Corte giust., 6 novembre 2003, Causa C-101/01, Gota Hovratt c. Lindqvist, *Danno resp.*, n. 4/2004, p. 377 ff. (in particolare, v. paragrafi 50-51 della motivazione); Cass., sez. un., 27 December 2017, n. 30981, *Rass. dir. civ.*, 2019, p. 266 ff., with commentary from Vivarelli, A.: "La tutela dei dati «sensibili» al vaglio delle Sezioni Unite", *ibid.*, p. 278 ff. 'Genetic data' are defined, on the other hand, by Article 4(13) as 'personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question'. For a commentary on this definition, see Bygrave, L.A., Tosoni, L., "Article 4(13). Genetic data", in C. Kuner, L.A. Bygrave, C. Docksey, (eds), cit., p. 196 ff. On this topic see Rodotà, S.: "Tra diritto e società. Informazioni genetiche e tecniche di tutela", *Riv. crit. dir. priv.*, 2000, p. 596 ff.; Laurie, G.: *Genetic Privacy: A Challenge to Medico-Legal Norms*, Cambridge, 2002; Gerards, J.H.: "General Issues concerning Genetic Information", in Id., A.W. Heringa, H.L. Janssen (eds), *Genetic Discrimination and Genetic Privacy in a Comparative Perspective*, Oxford, 2005, p. 5 ff.; Lattanzi, R.: "Ricerca genetica e protezione dei dati personali", in Aa.Vv., *Il governo del corpo*, I, in P. Zatti, S. Rodotà (eds.), *Trattato di biodiritto*, Milano, 2011, p. 319 ff.; Agnino, F.: "Nozione di dati genetici ed il decalogo di legittimità al loro trattamento", *Danno e resp.*, 2014, p. 43 ff.; Sirgiovanni, B.: "Informed Consent to Processing of Genetic Data", *ItaLJ*, 2022, p. 955 ff. In giurisprudenza, cfr. ECHR, 4 dicembre 2008, S e Marper c. Regno Unito, (*https://hudoc.echr.coe.int*).

of data' under Article 9(1) GDPR, the legal basis of the processing is increasingly found outside the data subject's consent.[16]

In this regard, it should be noted that, unlike in the past, the health professional, who is subject to professional secrecy, no longer has to request the patient's consent to data processing when this is necessary for the provision of the health service he/she has requested, regardless of whether the service is provided in a public or private health care facility.[17]

Moreover, national legislation provides under Articles 7(1) of Decree-Law No. 34 of 19 May 2020 and 2 sexies, paragraph 2(v), of the Code that the Ministry of Health may process without the consent of the data subjects 'personal data collected in the information systems of the National Health Service, including data relating to the health of patients, for the development of predictive methodologies of the evolution of the population's health needs'. This is a mine of personal data -

16 The hypotheses in which the processing of health data has as its legal basis the explicit consent given by the data subject for one or more specific purposes seem residual with respect to the other cases provided for in Article 9(2) GDPR and the Italian Privacy Code (henceforth: Code), in which the processing is necessary, and hereafter briefly indicated.
A) First, processing of health data that is necessary for reasons of substantial public interest in accordance with Article 9(2)(g) GDPR, i.e. performed by entities that carry out tasks in the public interest or in the exercise of official authority in the sectors identified in Italy by Art. 2 sexies of the Code, among which we highlight: welfare-related activities to protect children and frail, non-self-sufficient or incapacitated individuals; administrative activities and issuance of certifications in connection with health care and welfare activities (diagnosis, assistance, treatment) including organ and tissue transplantations and human blood transfusions; tasks committed to the national health service and health care practitioners; planning, management, monitoring and assessment of health care; oversight over experimental activities, pharmacovigilance, granting authorisations with a view to marketing and importing drugs and other health-relevant products; protection of motherhood, termination of pregnancy, handling of addictions, assistance to the disabled; processing activities for purposes of scientific research (see paragraph 2, sub-paragraphs *s* to *z*, *aa* and *cc*). Furthermore, paragraph 1-bis of Article 2-sexies provides for and legitimizes the processing of personal data relating to health, after removing directly identifying information, by the main actors of public health care in compliance with their respective institutional purposes, including the Ministry of Health, the Istituto Superioredi Sanità, the National Agency for regional healthcare services, the Italian Medicine Agency, the National Institute for the promotion of health in migrant populations and for the fight against poverty-related diseases, and Regions, also by way of the interlinking at national level of the individual information systems of the National Health Service including Electronic Health Records (FSE)
B) processing of health data for reasons of public interest in the area of public health referred to in Recital 54 and Article 9(2)(i) GDPR, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy (e.g. health emergencies following pandemics or food safety reasons)
C) processing operations referred to in Articles 9(2)(h) and (3) GDPR and 75 of the Code performed by (or under the responsibility of) a health professional subject to the obligation of professional secrecy or by another person also subject to the obligation of secrecy, for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with the health professional
D) the processing referred to in Article 9(2)(c) GDPR which is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

17 The Garante highlights this aspect: see Garante per la protezione dei dati personali, *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario - 7 marzo 2019*, web doc. n. 9091942; all measures and decisions of the Garante are available at *https://www.garanteprivacy.it*. See also Guarda, P.: "I dati sanitari", cit., p. 601.

much of which relates to the health of citizens - managed by the Ministry of Health for the purposes of so-called initiative medicine, within the framework of the 'New Health Information System' (NSIS), in compliance with specific pseudonymisation techniques[18] and within the limits of the provisions of paragraphs 2 and 2 bis of Article 7 of Legislative Decree No 34 of 19 May 2020[19].

The need for consent as a legal basis for the processing of health data remains, however, primarily for consultation of the FSE for the purposes of treatment, prevention and international prophylaxis pursuant to Article 12(2) and (5) of Italian Decree-Law No 179 of 18 October 2012, while consent to the feeding of the FSE has been cancelled by virtue of the repeal of paragraph 3-bis of the same Article[20]. Other cases in which the data subject's consent is required are listed in the Garante's decision of 7 March 2019[21]: by way of example, processing related to treatment, but not strictly necessary, even if carried out by health professionals; processing related to the use of medical Apps, also because the data subject's data can often be accessed by parties other than health professionals; processing aimed at customer loyalty, carried out by pharmacies or other providers of health products or services; health data processing carried out by private legal entities for promotional or commercial purposes. The definition of 'profiling' under Article 4(4) GDPR covers any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural

18 See Articles 2 and 3 of Ministerial Decree N° 262 of 7 December 2016 ("Regolamento recante procedure per l'interconnessione a livello nazionale dei sistemi informativi su base individuale del Servizio sanitario nazionale, anche quando gestiti da diverse amministrazioni dello Stato").

19 In fact, paragraph 2 of the aforementioned Article 7 provides for the adoption of a subsequent decree of the Minister of Health, subject to the opinion of the Garante, to identify the personal data (including those inherent to special categories of data under Article 9 GDPR) that can be processed, the operations that can be carried out, the methods of data acquisition and the appropriate and specific measures to protect data subjects' rights; while paragraph 2-bis clarifies that, pending the adoption of the aforementioned decree, the Ministry of Health shall initiate activities related to the classification of chronic diseases present in the Italian population, limiting them to the construction of analytical models prodromal to the realization of the predictive model of the population's health needs and ensuring that the data subjects shall not be directly identifiable.

20 The data subject must give his or her specific consent for each of the above purposes. In the first paragraph of Article 12 of Law Decree No. 179 of 18 October 2012, converted into Law No. 221 of 17 December 2012, the FSE is defined as the set of digital data and documents, of a health and social-health nature, concerning the patient and generated by present and past clinical events, also referring to services provided outside the National Health Service. [...] every healthcare service provided by public, accredited private and authorised private operators is entered in the FSE, within five days of the service itself. Paragraph 3-bis of the same Article 12 was repealed by Article 11(1)(d) of Decree-Law No. 34 of 19 May 2020, converted, with amendments, by Law No. 77 of 17 July 2020. Per piú ampi svolgimenti sul tema, v. Gambino, A.: "Riforma del fascicolo sanitario elettronico nell'emergenza sanitaria", in C. Petrini, C. D'Aprile, G. Floridia, S. Gainotti, L. Riva, S. Tamiozzo (eds.), *Tutela della salute individuale e collettiva: temi etico-giuridici e opportunità per la sanità pubblica dopo COVID-19*, Roma, 2020, p. 36 ff.; Gambino, A., Maggio, E., Occorsio, V.: "Il nuovo fascicolo sanitario elettronico: sottoscrizione, tutela dei dati, responsabilità civile", 22 luglio 2020 (*https://www.dimt.it/la-rivista/articoli/nuovo-fascicolo-sanitario-elettronico/*); Califano, L.: "Fascicolo sanitario elettronico (Fse) e dossier sanitario: il contributo del Garante privacy al bilanciamento tra diritto alla salute e diritto alla protezione dei dati personali", *Sanità pubblica e privata*, 2015, 3, p. 7 ff.; Comandé, G., Nocco, L., Peigné, V., "Il fascicolo sanitario elettronico: uno studio multidisciplinare", *Riv. it. med. leg.*, 2012, 105 ff.; Guarda, P.: *Fascicolo sanitario elettronico e protezione dei dati personali*, Trento, 2011.

21 See back, footnote 17.

person, including the purpose to analyse or predict aspects relating to his/her health.

III. SAFEGUARDS FOR THE PROCESSING OF HEALTH AND GENETIC DATA AND THE PRINCIPLE OF ACCOUNTABILITY.

In Italy, there are at least two factors that counterbalance this tendency to marginalise the role of data subject's consent to the processing of health data: one linked to the technical support activity carried out by the Garante and the other to a choice made by the legislator to bring domestic legislation into line with the GDPR.

With regard to the first aspect, the Garante provided some recent opinions to the Autonomous Province of Trento on specific draft regulations concerning initiative medicine in the provincial healthcare service.[22] The Garante intervened, in particular, on the issue of the lawfulness of data processing related to initiative medicine aimed at the prevention and early diagnosis of diseases. In this regard, it noted that this care model provides for the statistical risk stratification of patients, which is often carried out through the algorithmic processing of managed health data, aimed at profiling health service users in order to analyse and predict their health situation. The Garante has, therefore, established the need for data subjects' consent pursuant to Articles 9(2)(a) and 22 GDPR in order to provide a legal basis for the processing of health data aimed at creating a risk profile of the individual data subjects with reference to specific pathologies, since it is considered autonomous data processing with respect to that which is strictly necessary for the purpose of treatment under Article 9(2)(h).[23]

If, therefore, the processing of health data by the Ministry of Health for purposes of predictive or initiative medicine does not require the data subjects' consent, the same cannot be said for the processing of data by the regional and provincial healthcare system[24].

22 See the following opinions of the Garante: Garante per la protezione dei dati personali, 16 December 2021, n. 431, web doc. 9738538; 16 September 2021, n. 314, web doc. 3713993; 1 October 2020, n. 175, web doc. 9469372; 8 May 2020, n. 84, web doc. 9344635.

23 See Garante per la protezione dei dati personali, 15 December 2022, nn. 415, 416 e 417, web doc. 9844989, 9845156 e 9845312, paragraph 3.2; 8 May 2020, n. 84, cit., paragraph 3.2. In support of the contrary thesis that in such cases the legal basis of the data processing could be found outside the data subject's consent, it is noted that initiative medicine is a branch of precision or personalised medicine, so that the relevant data processing can be considered strictly necessary for purposes of diagnosis and patient care: Noce, S., Ottaviano, M.: "Medicina d'iniziativa, come renderla compliant al GDPR", 18 May 2022, available at *https://www.agendadigitale.eu/sicurezza/medicina-diniziativa-come-renderla-compliant-al-gdpr/*.

24 In this regard, see Garante per la protezione dei dati personali, 15 December 2022, n. 415, cit., paragraph 5.1.

As to the second aspect, the Italian legislator made use of the power granted to Member States by Article 9(4) GDPR to 'maintain or introduce further conditions, including limitations', with regard to the processing of data relating to health, genetic data or biometric data.[25] This rule leaves room for manoeuvre for Member States but poses problems. First of all, it entails a differentiation of guarantees and protections between Member States that may represent an obstacle to the free movement not only of health data, but also of health services in the European market.[26] Secondly, it is uncertain what is to be understood by 'further conditions' or 'limitations'. Some do not consider them relevant to the assessment of the lawfulness of processing.[27] On the contrary, a different interpretation seems to be preferred, which considers it possible for Member States to introduce additional conditions for the lawfulness of data processing when they are necessary to ensure the protection of data subjects' fundamental rights.

This is how we should understand the 'safeguards applying to the processing of genetic data, biometric data, and data relating to health' provided for in Article 2-septies of the Code, which refers their adoption to the Garante in compliance with the provisions of the same Article. In terms of content, the fifth paragraph specifies that 'the safeguards in question shall set out the security measures including encryption and pseudonymisation techniques, minimisation measures, the specific arrangements to enable selective access to the data and provide information to data subjects, and such additional measures as may be necessary to safeguard data subjects' rights': it is fair to doubt that the latter may also include the additional need to obtain the data subject's consent, in the absence of the specification to that effect contained in the sixth paragraph of the same Article for genetic data. In any case, where the safeguards take the form of technical and organisational measures, these should not be rigid or pre-packaged for all processing of these categories of data, but rather such as to be chosen and documented by the data controller, taking into account the specific purposes pursued and all the concrete circumstances, in line with the provisions of Article 24(1) GDPR and Article 2-septies of the Code[28].

25 On this article see Gerogieva, L., Kuner, C.: "Article 9. Processing of special categories of personal data", in Id., L.A. Bygrave, C. Docksey, (eds), *The EU General Data Protection Regulation*, cit., p. 372.

26 Guarda, P.: "I dati sanitari", cit., p. 600; cfr. Ferola L.: "Le 'misure di garanzia'", cit., p. 422 s.

27 On this topic see Pizzetti, F.: "La Parte I del Codice novellato", cit., p. 122 ff., who highlights the last part of the sixth paragraph of Article 2-septies of the Code where it is provided that 'as regards genetic data, the safeguards may provide for relying on the data subject's consent *as an additional measure to protect the data subject's rights […] pursuant to Article 9(4) of the Regulation*, or set out any additional specific precautions' (italics added): in this Author's view, this means that, in such cases, the failure to obtain consent does not determine the unlawfulness of the data processing, but only the failure to comply with a protection measure established in advance that can be considered as a security measure under Article 32 GDPR.

28 The first part of the fifth paragraph of Article 2-septies of the Code states that 'The safeguards shall be adopted in respect of each category of personal data as per paragraph 1 by having regard to the specific purposes of the processing and may lay down […] *additional conditions to be fulfilled for the processing of the said data to be allowed*' (italics added). That being said, it seems easy to assume that the failure to adopt the safeguards should result in the personal data processed being unusable under Article 2-decies of the Code

It should be noted here that the processing of health data presents a more pronounced declination of the principle of accountability, as well as of the principles of data minimisation, integrity and confidentiality. An indicative case in this sense is a decision of the Garante[29] sanctioning two local health authorities in the Friuli-Venezia Giulia Region for not having put in place all the necessary technical and organisational measures to prevent access to patient data by medical and nursing staff not involved in the treatment process. The Garante also sanctioned the IT company that manages the application for consulting online reports for failing to set up an alert system aimed at detecting anomalous or risky behaviour in relation to the operations carried out by the persons authorised to process data (e.g. the number of accesses, their type or time frame) and ordered the adoption of specific corrective measures.

One aspect that should not be underestimated is that - as expressly provided for in Article 2-septies, paragraph 2, of the Code - the Garante's provision on safeguards must take into account, first and foremost, the guidelines, recommendations and best practices published by the European Data Protection Board (EDPB) and the best practices concerning the processing of personal data, thus meeting the need for uniformity of regulation that is increasingly felt at European level; secondly, the scientific and technological developments in the sector addressed by the safeguards, given that the provision must be adopted every two years; and thirdly, the interest in the free movement of personal data within the Union, referred to in Article 1(3) GDPR.

IV. RECENT EVOLUTION OF DOMESTIC AND EUROPEAN LAW IN FAVOR OF SHARING AND REUSE OF HEALTH DATA: PREMISES FOR A POLICY OF DATA INTEGRATION AND INTEROPERABILITY.

The need to ensure the free movement of personal data within the Union cannot overshadow or sacrifice the goal of protecting the fundamental rights and freedoms of data subjects. This is precisely the most difficult and important challenge of our time.

In fact, the idea of favouring the sharing and re-use of personal and non-personal data is gaining ground in national and European law, even in the healthcare system that is being characterised as 'digital health'.[30].

and expose the data controller to the risk of having to pay compensation for any damage caused to the data subjects, pursuant to Article 82 GDPR.

29 See Garante per la protezione dei dati personali, *Dossier sanitario: il Garante privacy sanziona due Asl per accessi abusivi*, *Newsletter n. 493 del 26 luglio 2022*.

30 Section IV of the aforementioned Decree-Law No. 179 of 18 October 2012 is dedicated to 'Digital Health'. In EU legislation, the first reference to eHealth is Article 14 of Directive 2011/24/EU on the application of patients' rights in cross-border healthcare.

In this regard, the Italian National Recovery and Resilience Plan (PNRR) has intervened to enhance the FSE with investments on the following four objectives outlined in the "Guidelines" of March 27, 2022:[31]

«1. Access: A homogeneous FSE should be created throughout the country, representing the single and exclusive access point to SSN services for patients;

2. Integration: the FSE must become an effective tool for diagnosis and treatment, sharing relevant clinical data between professionals and healthcare facilities (public and private), guaranteeing continuity of care throughout the territory, and integrating with pharmacies in the definition of the treatment plan;

3. Personalisation: the quality and quantity of clinical data in the FSE must be increased in order to help health professionals in their capacity for personalised diagnosis and treatment;

4. Policy: a database on the health status of the population must be created to support both health institutions in the definition and implementation of prevention, health planning and governance policies, and research institutions for medical and biomedical research activities[32].

Integration and policy objectives are based on the principle of sharing health data within a network participated by public and private entities operating within the national health system. These tools have the dual purpose of improving the quality of services provided to patients, mostly with a view to personalisation, and of making (public) prevention and health planning policies more efficient and effective, as well as offering important support to scientific research in the medical and biomedical field. To this end, Article 12, paragraph 15-ter of Law Decree No. 179/2012, provided for the creation of a National Portal and an FSE Infrastructure - the National Infrastructure for Interoperability or INI - which is a repository of clinical data and documents, capable of interoperating with the information systems

31 "Linee Guida per l'Attuazione del Fascicolo Sanitario Elettronico", 27 March 2022, in G.U. 11 July 2022, n. 160. The procedures for the adoption of this document are provided for in Article 12, paragraph 15 bis of Law Decree No. 179/2012. However, the Garante noted that the aforementioned Guidelines were adopted prior to the new decree aimed at regulating the FSE, contrary to the provisions of the aforementioned Article 12, paragraph 15 bis. Moreover, almost in parallel with the publication of the Guidelines, the Garante expressed a negative opinion on the first draft decree on the FSE with the following opinion to the Ministry of Health: Garante per la protezione dei dati personali, 22 August 2022, no. 294, web doc. 9802729. A second draft decree was then drafted, on which the Garante expressed a positive opinion: see Garante per la protezione dei dati personali, 8 June 2023, no. 256, web doc. 9900433. Finally, on 2 August 2023, the draft decree received the favourable opinion of the State-Regions Conference and is therefore about to enter into force.

32 "Linee Guida per l'Attuazione del Fascicolo Sanitario Elettronico", cit., p. 59. Moreover, in a recent decision, the Garante stated that the FSE does not have the nature of a public act as it does not certify an individual's state of health, but rather provides, in a potentially incomplete manner, health information that may facilitate the course of treatment; the FSE is therefore configured as a mere tool for retrieving part of the data and documents relating to an individual's health history with the aim of providing a general scenario of the individual's health to the health professionals taking care of him/her, who are not however obliged to consult it or feed it.: see Garante per la protezione dei dati personali, 22 August 2022, n. 294, cit., paragraph 1.2.

in use at the various territorial healthcare facilities, as well as with the systems that manage data on organ donation, vaccinations and bookings. This infrastructure will be aligned with the ANA (National Registry of Assisted Persons) and with the National Registry of Consents and Consent Revocations. Moreover, Article 12, paragraph 15 quater, of Law Decree 179/2012 provides for the creation by the Ministry of Health of an Ecosystem of Health Data (EDS) intended to operate according to the logic of an integrated management of health data, based on their interoperability: this need has emerged especially in the recent pandemic period.[33] The implementation of the EDS has been hindered by a recent negative opinion of the Garante on a draft decree designed to identify its contents, how it is to be fed, who is authorised to access it, what operations can be carried out and what security measures can be taken.[34]

With respect to these ambitious goals, the role of the Garante is essential in presiding over the implementation of the principles of the GDPR, so as to direct and define, with its prior opinions , a more detailed policy on the protection of personal data and the protection of the fundamental rights and freedoms of data subjects[35]. Garante's decisions have had an impact especially with regard to identifying the roles and responsibilities of those involved in data processing, selecting how health data can be accessed by those who are authorized, defining the requirements for lawfulness and transparency as well as the technical and organizational security measures that must be taken.

V. THE 'EUROPEAN STRATEGY FOR DATA', THE F.A.I.R. PRINCIPLES AND THE SECONDARY USE OF HEALTH DATA FOR SCIENTIFIC RESEARCH PURPOSES.

The goal of establishing a national health data ecosystem should be placed in the context of a broader strategic vision set out atthe European Union level

33 On this point, see paragraph 1 of the Explanatory Memorandum of the 'Proposal for a Regulation of the European Parlament and of the Council on the European Health Data Space', Strasbourg 3.5.2022, COM(2022) 197 final, available at: *https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=CELEX:52022PC0197*. See Resta, G.: "La protezione dei dati personali nel diritto dell'emergenza Covid-19", *Giustizia Civile.com Emergenza Covid-19 Speciale n.3*, p. 522 ff., who emphasises the numerous measures taken by the Italian Government to encourage the sharing and integrated use of health data in the context of the pandemic response.

34 See Garante per la protezione dei dati personali, 22 agosto 2022, n. 295, web doc. 9802752. In this opinion on the draft decree, the Garante notes that the EDS represents the largest health data bank in Italy, in which to collect, without applying any pseudonymization techniques, the health data and documents of all patients related to the social-health services provided on the national territory, including through algorithmic logics, with high risks for the rights and freedoms of the data subjects. According to the Garante, the said model has a number of critical elements regarding personal data protection, so the relevant draft decree needs to be reformulated.

35 In this regard, the Garante pointed out that its prior opinion has not been requested with respect to the adoption of some ministerial decrees having important implications on the protection of personal data in the healthcare system. Such is, for example, the case of Ministerial Decree 21 September 2022, containing guidelines for telemedicine services, in which there is no reference to the processing of personal data: Garante per la protezione dei dati personali, 8 June 2023, cit.

by the Commission in its February 19, 2020, Communication on "A European Strategy for Data"[36].

It should be premised that this communication envisions the creation of a European Health Data Space. However, before considering this aspect, it is appropriate to examine in more detail the aims and principles behind the strategy outlined by the European Commission.

First, the Commission states that «[t]he aim is to create a single European data space – 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 […] Data spaces should foster an ecosystem (of companies, civil society and individuals) creating new products and services based on more accessible data».[37]

The new European strategic vision seems to be moving toward a more market-centric approach to the use of personal data, which are to be understood as a resource for the creation of new products and services, as well as a tool for business development and, therefore, economic growth. At the same time, it is significant that the text of the 'Strategy' almost entirely preempts the use of the term (and notion of) 'processing' around which the GDPR framework is built, and that it appears here to be almost absorbed or dissolved into the notion of 'data space', i.e. a 'genuine single market' comprising data-sharing architectures and federated or interconnected cloud infrastructures where all data – especially personal data – 'are secure'.

The kind of cultural approach and strategic design targeted by the Union institutions take a more defined form in the four pillars on which the 'Strategy' is based. Of these, the first, which consists of the establishment of a 'cross-sectoral governance framework for data access and use', and the fourth, relating to the creation of a 'Common European data spaces in strategic sectors and domains of public interest', are particularly important.[38]

With a view to the implementation of an enabling legislative framework for the governance of common European data spaces, the Commission made clear its preference for 'an agile approach [...] that favours experimentation [...] and

36 On this important document, see back, footnote 1.

37 See Communication from the Commission, *A European Strategy for Data*, cit., paragraph 3.

38 The 'four pillars' underpinning the European data strategy are: A) A cross-sectoral governance framework for data access and use; B) Enablers: Investments in data and strengthening Europe's capabilities and infrastructures for hosting, processing and using data, interoperability; C) Competences: Empowering individuals, investing in skills and in SMEs; D) Common European data spaces in strategic sectors and domains of public interest.

differentiation', abstaining from 'overly detailed, heavy-handed *ex ante* regulation'[39]. This process is being implemented in line with the new and essential principles on Findability, Accessibility, Interoperability and Reusability (hereafter: FAIR principles) of data, which will have to coordinate and integrate with the GDPR principles. This approach is based on the central idea that 'the value of data lies in its use and re-use'[40] and, with specific regard to the health system, the goal of creating in the Union a reference model in the management and sharing of electronic health data, in order to exploit its full potential, both in the delivery of care and assistance services to citizens (primary use of data) and in the secondary use of data[41].

To be honest, a 'secondary use' is already possible for all personal data, in the sense that it is possible to use the data for a purpose other than the one for which it was originally collected and processed (so-called primary use: e.g., for health care purposes). This possibility is allowed by the GDPR in order to give greater flexibility to the principle of purpose limitation, albeit subject to a compatibility test that is stricter for sensitive data and is governed by Article 6(4), which requires taking into account, among other things, the nature of the personal data and the existence of appropriate safeguards.[42]

Regarding the secondary use of health data, the most relevant purpose seems to be that which pertains to scientific research purposes in the medical, biomedical and epidemiological fields[43]. Articles 5(1)(b), 9(2)(j) and 89 GDPR, 110 and 110-bis

39 See Communication from the Commission, *A European Strategy for Data*, cit., paragraph 'A. A cross-sectoral governance framework for data access and use'.

40 This statement can be found in Communication from the Commission, *A European Strategy for Data*, cit., paragraph 4.

41 On this point see Cabrio, A.: "La seconda vita dei dati. Luci e ombre della normativa privacy in materia di secondary data use", in F. Frattino, F. Massimino (eds.), *I dati. Il futuro della sanità. Strumenti per una reale innovazione*, Milan, 2022, p. 25.

42 Pursuant to Recital 50 of GDPR, «[i]n order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations». See also Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation - Adopted on 2 April 2013*, p. 20 ff. On this topic, see Becker, R., Comandé, G., et Al., *Secondary Use of Personal Health Data*, cit.; Modafferi, F.: "Il regime particolare dei trattamenti dati effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri", in F. Pizzetti (ed.), *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, cit., p. 397 ff.

43 In this regard, Recital 159 of GDPR specifies that 'the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health'. On this topic see European Commission, *Study on Health Data, Digital Health and Artificial Intelligence in Healthcare*, Luxembourg, 2022; Id., *Assessment of the EU Member States' rules on health data in the light of GDPR*, Luxembourg, 2021; Garante per la protezione dei dati personali, *Applicare il GDPR. Le linee guida europee*, Rome, 2019, p. 43 ff. In the literature, see Dierks, C., Kircher, P., Husemann, C., Kleinschmidt, J., and Haase, M.: *Data Privacy in European Medical Research: A Contemporary Legal Opinion*, Berlin, 2021; Wiese

of the Code and the measures of the Garante concur to regulate the processing of data for these purposes and go in the directions of limiting the need for data subjects' consent to certain cases[44], or allowing special ways of providing consent in relation to the specificities of research projects[45], and encouraging the secondary use of health data by (public or private) third parties, who primarily carry out research activities, without requiring a new consent as a legal basis. In such cases, appropriate measures and adequate safeguards for the fundamental rights and freedoms of data subjects must be taken in advance, and in addition, where data subjects cannot be informed due to special reasons, prior intervention by the Garante in the form of individual or general authorization is also necessary[46].

One issue of particular interest concerns the secondary use of data on the health of individuals participating in nonprofit research projects or clinical trials by corporations or other for-profit entities operating in the private health care sector,

Svanberg, C.: "Art. 89. Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes", in C. Kuner, L.A. Bygrave, C. Docksey, (eds), *The EU General Data Protection Regulation*, cit., p. 1240 ff.; Resta, G.: "Biobanche, ricerca scientifica e tutela della persona", in P. Perlingieri et al. (eds.), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, Napoli, 2020, p. 41 ff.; Malgieri, G.: "Data protection and research: A vita challenge in the era of Covid-19 pandemic", *Computer Law & Security Rev.*, 2020, p. 1 ff.; Ducato, R.: "Data protection, scientific research, and the role of information", *ibid.*, p. 2 ff.; Uda, G.M.,: "Il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricercar scientifica o storica o a fini statistici", in V. Cuffaro, R. D'Orazio, V. Ricciuto (eds.), *I dati personali nel diritto europeo*, cit., p. 569 ff.

44 In fact, the explicit consent of the data subject is, as a rule, necessary when the primary use of health data coincides with processing for scientific research purposes, in the sense that they are directly collected and processed for this purpose. Consent to data processing should not be confused with informed consent to participate in research, which is provided for in the relevant regulations. However, pursuant to Articles 110 of the Code, 9(2)(j) and (4) GDPR, such a lawfulness prerequisite is not necessary if informing the data subjects proves impossible or entails a disproportionate effort on specific grounds, or if it is likely to render impossible or seriously impair the achievement of the research purposes. In such cases, the controller shall take appropriate measures to protect the rights, freedoms and legitimate interests of the data subjects and the research programme shall be the subject of a reasoned, favourable opinion by the geographically competent ethics committee as well as being submitted to the Garante for prior consultation in accordance with Article 36 of the GDPR. On making a distinction between the primary use of health data for scientific research purposes and their secondary use for the same purposes, see European Commission, *o.c.*, p. 57. For some examples of measures rendered by the Garante under Articles 110(1) of the Code and 36 GDPR, see Garante per la protezione dei dati personali, 30 June 2022, n. 238, web doc. 9791886; e 1° November 2021, n. 406, web doc. 9731827.

45 In principle, scientific research projects can only include personal data on the basis of consent if they have a well-described purpose. However, it is exceptionally provided that, when research purposes cannot be fully specified, a controller must seek other ways to ensure the essence of the consent requirements are served best, for example, to allow data subjects to consent for a research purpose in more general terms and for specific stages of a research project that are already known to take place at the outset. As the research advances, consent for subsequent steps in the project can be obtained before that next stage begins. Yet, such a consent should still be in line with the applicable ethical standards for scientific research: in this regard see EDPB, Guidelines 05/2020 on consent under Regulation 2016/679 - *Adopted on 4 May 2020*, points 156-159. See also Garante per la protezione dei dati personali, 30 June 2022, n. 238, cit., paragraph 4.1.

46 On this point, reference is made to the provisions of Article 110 bis (2) and (3) of the Code. It follows from the article that the further processing of health data for scientific research purposes normally requires not the data subjects' consent, but rather that the data subjects be given adequate information to enable them to exercise their rights. Only where this is not possible, the Garante's authorization would become necessary, although this mechanism seems to be translatable into compliance with the 'Prescriptions concerning the processing of personal data carried out for scientific research purposes' under Appendix 1, paragraph 5, of the following decision of the Garante: Garante per la protezione dei dati personali, 13 December 2018, n. 497, web doc. 9068972. On this topic see Cabrio, A., *La seconda vita dei dati*, cit., p. 26 ff.

particularly for commercial purposes inherent in the pharmaceutical market. The problem arises, for example, with respect to the contract for the transfer of data from nonprofit clinical trials, as well as their results, for the purpose of placing one or more drugs on the market; such a contract is, as a rule, concluded between the principal investigator of the clinical trial and the company interested in the secondary use of the data[47]. In fact, the regulation of this contract - set forth in Article 3 of the Ministry of Health's Decree of November 30, 2021[48] - expressly provides that '[p]ursuant to the transfer, the transferee takes over for all purposes the processing of personal data related to the trial', without anything else specifying regarding the legal basis of the data processing. In this regard, neither the circumstance that - for the purposes of the GDPR - the notion of 'scientific research' includes 'privately funded research' (see recital 159), nor, more generally, the favoring of 'data reuse' at the European level seem sufficient arguments in themselves to deem it unnecessary to acquire new consent for processing from data subjects, where possible[49].

In this respect, taking into account the particularly sensitive nature of health data, equating the secondary use of such data for purposes of general interest such as scientific research or nonprofit experimentation, on the one hand, with the reuse of data for activities instrumental to the pursuit of industrial or commercial purposes by private parties, on the other, should not be possible, since only in the second case should autonomous processing be configured[50]. It follows that it should be better to apply, by analogy, Article 110 of the Code rather than Article 110 bis to the processing underlying the data transfer contract, with the result that it would be necessary to acquire new consent from the data subjects unless informing them of the data transfer proves impossible or involves a disproportionate effort: in the latter case, it would perhaps be appropriate to impose the anonymization of health data[51]. Moreover, recent studies have shown that, although the European

47 On this topic see Piria, C.A., "Aspetti contrattuali delle sperimentazioni cliniche no-profit", *Contratti*, 2022, p. 346 ff.; Cabrio, A.: *ibid*.

48 This is the Ministerial Decree of 30 November, 2021, "Misure volte a facilitare e sostenere la realizzazione degli studi clinici di medicinali senza scopo di lucro e degli studi osservazionali e a disciplinare la cessione di dati e risultati di sperimentazioni senza scopo di lucro a fini registrativi, ai sensi dell'art. 1, comma 1, lettera c) del decreto legislativo 14 maggio 2019, n. 52". The decree entered into force on March 3, 2022.

49 On this argument, see Cabrio, A.: *ibid*.

50 In this regard, compare the well-known Tiziana Life vs. Garante Privacy case, on which the Italian Supreme Court finally ruled, upholding the argument of the Garante, which had found legitimate the withdrawal of consent (under Directive 95/46) asserted by Sardinian citizens of Ogliastra against the company that had purchased, for consideration, their biological samples: Cass., ord., 7 October 2021, n. 27325, *Nuova giur. civ. comm.*, 2022, p. 590 ff., con il commento di Corti, D.: "La sorte (incerta) della ricerca sui campioni biologici umani all'indomani della decisione Shardna", *ibid*., p. 594 ff. The above case relates to the transfer of a bank of sensitive data, including genetic data, in the force of the Code in the version prior to the amendments introduced by Legislative Decree No. 101 of August 10, 2018, adapting to the GDPR. The Supreme Court affirms, among other things, the principle of the indispensability of informed consent in the case of the transfer of a genetic database, where the exceptions provided by law do not apply.

51 Where Article 110 of the Code is deemed applicable by analogy, in those cases where the new consent cannot be acquired from the data subjects, the data transferee, as the new data controller, should take

public is generally supportive of the reuse of health data, there are significant concerns when the data are used by commercial entities. A survey among rare disease patients indicated that while they have high confidence in academic and not-for-profit organisations re-using data for research, they are less confident when data are used for research by governmental or commercial organisations[52].

VI. THE 'ALTRUISM OF DATA' AND THE GOAL OF CREATING A EUROPEAN COMMON HEALTH DATA SPACE.

In the context of the European data strategy, the re-use of personal health data in the healthcare system tends to be, especially for the future, an expression of an altruistic or solidaristic approach to the use of personal data and the right of each person to informational self-determination[53]. In fact, EU Regulation 2022/868 of 30 May 2022 on European data governance (or 'Data Governance Act') encourages 'data altruism'[54] whereby data subjects will be able to consent to the processing of personal data concerning them for purposes of general interest, such as healthcare, improving the quality of public services or public policies, and supporting scientific research. This may contribute to the development, on a voluntary basis, of 'pools' or 'repositories' of data on such a scale that they can be analysed by means of algorithmic processing and machine learning processes. Their creation and management will be entrusted to 'Union-recognised data altruism organisations', i.e. non-profit bodies with specific requirements to establish trust and credibility in public opinion.[55] With regard to the health system, it should be

appropriate measures to protect the rights, freedoms and legitimate interests of the data subject and, most importantly, the data transfer should be subject to prior consultation with the Garante under Article 36 of the GDPR.

52 Courbier, S., Dimond, R., Bros-Facer, V.: "Share and protect our health data: an evidence based approach to rare disease patients' perspectives on data sharing and data protection - quantitative survey and recommendations", *Orphanet Journal of Rare Diseases*, 2019, p. 175.

53 In the Communication on "A European Strategy for Data", the Commission states that one of the issues that the new legislative and governance framework proposes to address is to 'make it easier for individuals to allow the use of the data they generate for the public good, if they wish to do so ('data altruism'), in compliance with the GDPR'.

54 Under Article 2 of the Data Governance Act, 'data altruism' means 'the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest'.

55 In this regard, see the framework contained in Articles 16 to 25 of Regulation 2022/868 and Recitals 45-46 where it is specified that the above-mentioned requirements of organisations for data altruism should include 'making it possible to process relevant data within a secure processing environment […] oversight mechanisms such as ethics councils or boards, including representatives from civil society to ensure that the data controller maintains high standards of scientific ethics and protection of fundamental rights, effective and clearly communicated technical means to withdraw or modify consent at any moment […] as well as means for data subjects to stay informed about the use of data they made available'. The same Regulation defines a 'secure processing environment' as 'the physical or virtual environment and organisational means to ensure compliance with Union law, such as Regulation (EU) 2016/679, in particular with regard to data

avoided that the health data pools thus constituted represent multiple duplications of data already present in the EDS or the NSIS, with the consequence of increasing the risks for the fundamental rights of data subjects without any significant benefit for the community.

In accordance with the FAIR principles, the Data Governance Act has also intended to promote the 'availability' of certain categories of data stored in public databases for which re-use is more difficult (e.g., because they are protected by data protection legislation, intellectual property or trade secrets or other commercially sensitive information); it has, therefore, strengthened data sharing mechanisms on a voluntary basis throughout the Union by facilitating 'government-to-business, G2B data sharing'[56]. The sharing mechanisms under this regulation will require strict compliance with the principles and rules of the GDPR for health data managed by regional and provincial health systems and the National Health System, where permitted.[57].

It should be noted that, within the aforementioned framework of new European principles, one of the strategic areas in which a European data space will be created is the health sector: 'a common European health data space, which is essential for advances in preventing, detecting and curing diseases as well as for informed, evidence-based decisions to improve the accessibility, effectiveness and

subjects' rights, intellectual property rights, and commercial and statistical confidentiality, integrity and accessibility, as well as with applicable national law, and to allow the entity providing the secure processing environment to determine and supervise all data processing actions, including the display, storage, download and export of data and the calculation of derivative data through computational algorithms'.

56 On the '*Use of public sector information by business (government-to-business – G2B – data sharing)*' see paragraph 4 of the European Commission Communication on 'A European Strategy for Data', where the problem is highlighted that 'sensitive data (e.g. health data) in public databases is often not made available for research purposes, in the absence of capacity or mechanisms that allow specific research actions to be taken in a manner compliant with personal data protection rules'. Furthermore, in 'Chapter II: Solidarity and Inclusion' of the 'European Declaration on Digital Rights and Principles for the Digital Decade' of 26 January 2022, the European Parliament, the Council and the Commission committed themselves to 'ensuring wide accessibility and re-use of public sector information'.

57 The Data Governance Act makes it clear that the sharing of personal data still requires a legal basis and compliance with the conditions laid down in the GDPR. In this regard, Recital 15 provides the following: '[…] Conditions attached to the re-use of data should be designed to ensure effective safeguards with regard to the protection of personal data. Before transmission, personal data should be anonymised, in order not to allow the identification of the data subjects, and data containing commercially confidential information should be modified in such a way that no confidential information is disclosed. Where the provision of anonymised or modified data would not respond to the needs of the re-user, subject to fulfilling any requirements to carry out a data protection impact assessment and consult the supervisory authority pursuant to Articles 35 and 36 of Regulation (EU) 2016/679 and where the risks to the rights and interests of data subjects have been found to be minimal, on-premise or remote re-use of the data within a secure processing environment could be allowed.
This could be a suitable arrangement for the re-use of pseudonymised data. Data analyses in such secure processing environments should be supervised by the public sector body, so as to protect the rights and interests of third parties. In particular, personal data should be transmitted to a third party for re-use only where a legal basis under data protection law allows such transmission. […] the public sector body should make best efforts to provide assistance to potential re-users in seeking such consent or permission by establishing technical mechanisms that permit transmitting requests for consent or permission from re-users, where practically feasible. […]'.

sustainability of the healthcare systems'[58]. Among the most important innovations envisaged by the proposal for a regulation on the European health data space, recently drawn up by the European Commission[59], a common infrastructure - called 'MyHealth@EU' for the primary use of electronic health data, and 'HealthData@EU' for their secondary use - is designed to facilitate cross-border exchange, portability and sharing of electronic health data, also through the setting up of 'health data access bodies' (appropriately coordinated among themselves) by the Member States[60].

VII. PROBLEMS AND NEW CHALLENGES OF THE RECENT EUROPEAN APPROACH TO DATA GOVERNANCE IN HEALTHCARE.

It is not easy to combine the FAIR principles with the idea that the protection of people in their fundamental rights remains the central element in the Union's policies, as also stated in the 'European Declaration on Digital Rights and Principles for the Digital Decade'.[61]

The problems to be tackled with regard to health data are numerous and complex, and the solutions put forward are not always timely and adequate.

In the area of private healthcare, there are widespread commercial practices related to the apparently free offer to consumers of applications to monitor their health status, and to health professionals of applications and software for processing or segmentation of diagnostic images that involve the sharing of health data of a very large number of patients with companies based outside the EU.[62] It

58 See Communication from the Commission, 'A European Strategy for Data', cit., paragraph 5, point 'D. Common European data spaces in strategic sectors and domains of public interest'. Furthermore, paragraph 4 of the Appendix to the Communication is dedicated to the 'Common European Health Data Space': the Commission emphasises the centrality of this objective in order to make sure 'that every citizen has secure access to their Electronic Health Record (EHR) and can ensure the portability of his/her data within and across borders', which 'will improve access to and quality of care, cost effectiveness of care delivery and contribute to the modernisation of health systems'. To this end, the Commission will 'support the development of national electronic health records (EHRs) and interoperability of health data through the application of the Electronic Health Record Exchange Format. Scale up cross-border exchange of health data; link and use, through secure, federated repositories, specific kinds of health information, such as EHRs, genomic information (for at least 10 million people by 2025), and digital health images, in compliance with the GDPR'.

59 Reference is made to the 'Proposal for a Regulation of the European Parlament and of the Council on the European Health Data Space', cit. On this draft, for more details on the issue of its compliance with the GDPR, see il "EDPB-EDPS Joint Opinion 3/2022", adopted on 12 July 2022, available at *https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf*.

60 In this regard, see Recitals 24, 25, 26, 55 and Articles 2(1)(t) and (x), 12, 13, 52, 53, 54 of the above Proposal for more details.

61 See the title of Chapter I of the 'European Declaration on Digital Rights and Principles for the Digital Decade': 'Putting people at the centre of the digital transformation'.

62 For example, see the following scientific article comparing some software available to health professionals, using a number of technical evaluation parameters that neglect, however, the profile of their actual adequacy in terms of data protection: Virzì, A., et al., "Comprehensive Review of 3D Segmentation Software Tools for MRI Usable for Pelvic Surgery Planning", *Journal of Digital Imaging*, 2020, p. 99 ff.

is true that the 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data' (or Data Act)[63] aims to intervene on these aspects: this regulation will give users and companies the possibility to decide on how the data - including health-related data - generated by their products or related services can be used. However, *rebus sic stantibus*, the agreements underlying the free use of the aforementioned software are, in most cases, outside the perimeter of legality established by European data protection rules, with high risks of unfair relationships and violation of data subjects' rights.

Another problematic aspect is that the support actions for the development of interoperable European data spaces envisage heavy investment in federated cloud infrastructures with architectures and governance mechanisms for data sharing ecosystems and Artificial Intelligence (AI)[64]. In this context, the legal basis of algorithmic processing of health data is uncertain, although some identify it in Articles 9(1)(j) and 89 GDPR. However, it is also a phenomenon that hides high risks of dehumanisation of the doctor-patient relationship and of discriminatory conduct[65] or, in any case, of conduct detrimental to the fundamental rights of the persons involved, especially in relations with other subjects or private powers: one thinks of the use of metadata derived from algorithms, predictive of probable future health conditions referring to certain groups or communities, in the insurance sector or in personnel selection processes. In order to tackle these risks, the proposal for a regulation on the European health data space provides in Article 35 for the prohibition of the secondary use of electronic health data both to take decisions in relation to a natural person or groups of natural persons to exclude them from the benefit of an insurance contract or to modify their contributions and insurance premiums; and, more generally, to take decisions detrimental to a natural person, such as to produce legal effects or affect him/her in a similar significant way.

63 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data', 23 February 2022, COM(2022) 68 final, (*https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN*).

64 On this topic see Mayer-Schönberger, V., Ingelsson, E., "Big Data and Medicine - a Big Deal?", *Journal of Internal Medicine*, 2018, p. 283 ff.; Price, W.N., Cohen, I.G.: "Privacy in the Age of Medical Big Data", *Nature Medicine*, 2019, p. 25 ff.; Perlingieri, C.: "Responsabilità civile e robotica medica", *Tecn. Dir.*, 2020, p. 161 ff.; Vimercati, F.: "Intelligenza artificiale in sanità", in P. Perlingieri, S. Giova e I. Prisco (eds.), *Rapporti civilistici e intelligenze artificiali: attività e responsabilità*, Naples, 2020, p. 211 ff.; Cerea, F.: "Intelligenza artificiale a servizio dei pazienti per il contrasto a CoViD-19", *Nuova Giur. Comm.*, 2020, suppl., p. 45 ff.; Rauccio, C.: "Artificial intelligence and genomics: the Data protection implications in the use of AI for genomic diagnostics", *Eur. J. Privacy Law Tech.*, 2021, p. 115 ff. In a more general perspective see Comandé, G.: "Leggibilità algoritmica e consenso al trattamento dei dati personali, note a margine di recenti provvedimenti sui dati personali", *Danno resp.*, 2022, p. 141 ff.; Amram, D.: "The Role of the GDPR in Designing the European Strategy on Artificial Intelligence: Law-Making Potentialities of a Recurrent Synecdoche", *Opinio Juris in Comp.*, 1, 2020, p. 1 ff.; Pizzetti, F.: "La protezione dei dati personali e la sfida dell'Intelligenza Artificiale", in Id. (ed.), *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Turin, 2018, p. 5 ff.; Zarsky, T.Z.: "Incompatible: The GDPR in the Age of Big Data", *Seton Hall Law Review*, 2017, p. 47 ff.

65 In this regard see Zuiderveen Borgesius, F.J.: "Strengthening legal protection against discrimination by algorithms and artificial intelligence", *The International Journal of Human Rights*, 2020; Hacker, P., "Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law", *Common Market Law Review*, 2018, p. 1143 ff.

With regard to the protection of personal data, the need to cope with risks relating to the confidentiality and integrity of an enormous amount of potentially accessible sensitive electronic data should lead one to conceive of the data space effectively as a 'secure processing environment', in the sense indicated by Article 50 of the proposal for a regulation on the European health data space[66]. The question arises whether this technical and legal notion is adequate for the purpose and the underlying risks.

In order to ensure control of personal data in this changed context, the European Data Strategy points to other tools, where it foresees the goal of fostering the development and use of 'personal information management apps, including fully decentralised solutions building on blockchain', as well as 'personal data cooperatives or trusts' and 'novel data intermediaries such as providers of personal data spaces' guaranteeing their role as neutral brokers in the personal data economy.[67]

It will, however, take time for these new intermediary service providers to establish themselves in the market.

To prevent a dangerous market-centric drift, the main effort to be made must be in the direction of a correct application of the GDPR principles, in particular their balancing and coordination with the new European data governance principles.

The principle of accountability should assume a central role with respect to the algorithmic processing of electronic health data, since this principle requires the data controller to carry out a prior assessment of the risks to the rights of all the subjects involved in the processing chain and, on the basis of this impact assessment, to adopt technical and organisational measures appropriate to the concrete risks. In this perspective, it becomes crucial to establish upstream the data quality criteria on the basis of which the analyses will be developed, as well as the purposes and the logic underlying the processing methods, so that they are transparent and subject to a critical scientific and legal control[68].

66 With reference to a 'secure processing environment', this article provides for the adoption of particular security measures, including: restrict access to authorised persons; minimise the risk of the unauthorised reading, copying, modification or removal of electronic health data; limit the input of electronic health data and the inspection, modification or deletion of electronic health data to a limited number of authorised identifiable individuals; ensure that data users have access only to the electronic health data covered by their data permit, by means of individual and unique user identities and confidential access modes only; keep identifiable logs of access for the period of time necessary to verify and audit all processing operations.

67 For more details on these new services that will be offered in the digital market, see recitals 30 to 44 and Article 2(11) and (15) of the Data Governance Act, where the notions of 'data intermediation service' and 'services of data cooperatives' are defined respectively, as well as see Articles 10 to 14.

68 On this point see Comandé, G.: "Leggibilità algoritmica e consenso", cit.

The measures adopted must then be inspired by the principles of privacy by design and privacy by default and take into account available technologies that can be used to minimise risks (e.g. blockchain).

The principle of data minimisation provides an opportunity to assess another aspect that is fundamental to the development of the digital economy and the proper functioning of the European and internal health data space: the anonymisation of personal data[69]. Further studies and research need to be conducted in the health sector to establish how to anonymise diagnostic images in a legal sense and better clarify the boundaries with regard to pseudonymisation. This seems to be perhaps the most effective means of protecting the data subjects and pursuing the objectives of research development and those set out in the European Data Strategy, unless the development of personalised medicine leads to a different hierarchy of interests and values.

With regard to the risks linked to the dominance of algorithmic decisions and the robotization of the care relationship[70], here too the solution on a legal level is provided by the GDPR, since Article 22(1) establishes the principle that the data subject has the right not to be subjected to a decision based solely on automated processing that produces legal effects concerning him or significantly affects him. Moreover, exceptions to this principle are more limited when decisions are based on special categories of personal data (including health data), as provided for in the last paragraph of the same Article[71]. The right to human intervention (by the doctor) in the decision to diagnose and treat is, therefore, an inescapable right of the patient and must continue to be so in the future.

One of the turning points of the European Data Strategy is the solidaristic approach to the objective of promoting the re-use of data, especially in the health

69 Anonymisation techniques are a rather complex subject, as can be seen from a number of recent decisions of the Garante concerning the health sector: see Garante per la protezione dei dati personali, 1° June 2023, n. 226, web doc. 9913795; 15 December 2022, n. 416, cit. In both decisions, the Garante makes it clear that anonymisation cannot be considered to be achieved through the mere removal of the personal details of the data subject or their replacement by a pseudonym code; and that 'an anonymisation process cannot be defined as effectively anonymous if it is not suitable for preventing anyone using such data, in combination with "reasonably available" means, from (1) isolate a person in a group (single-out); (2) link an anonymised data to data referable to a person in a separate data set (linkability); (3) infer new information referable to a person from an anonymised data (inference). See also the 'Opinion 05/2014 on Anonymisation Techniques' adopted on 10 April 2014 by the Article 29 Data Protection Working Party, available at *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf*; in the literature see D'Acquisto, G., Naldi, M.: *Big Data e privacy by design. Anonimizzazione Pseudonimizzazione Sicurezza*, Turin, 2017, p. 41 ff.

70 On the topic of medical robotics see Perlingieri, C.: "Responsabilità civile e robotica medica", cit., p. 178 s., who observes that, with the use of neurobotic technologies such as wetware systems, in the therapeutic relationship there could be that empathy that today seems excluded by algorithm-based Artificial Intelligences. On the risks linked to the dominance of algorithmic decisions, see Noto La Diega, G.: "Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information", *JIPITEC*, 2018, 9, p. 1 ff.

71 For more details, see Bygrave, L.A.: "Art. 22 Automated individual decision-making, including profiling", in C. Kuner, L.A. Bygrave, C. Docksey, (eds), *The EU General Data Protection Regulation*, cit., p. 539.

sector. The term 'data altruism' has been used in preference to the term 'data donation' as the latter implies ownership transfer and the concept of ownership does not fit comfortably with health data which are 'about the patient' as a centre of relevant interests, but do not 'belong to the patient'. Furthermore, 'the concept of ownership could even be harmful to the promotion of the notion of data altruism, as ownership (and therefore the passing of ownership to another) risks severing of the connection between the patient and their data'.[72] It is also true that the persons or entities that are the term of reference for interests or rights in personal data are no longer only the data subject and the data controller, but also - according to the Data Governance Act - the 'data holder', who/which 'has the right to grant access to or to share certain personal data or non-personal data', and the 'data user', who/which has legitimate access to certain data, including personal data, and the right to use them for commercial or non-commercial purposes.[73]. The reference here is to the possibility for small and medium-sized enterprises to have access to a wealth of information, hitherto reserved for large multinationals, through which they can be more competitive and exploit new development opportunities.

It follows that the 'pillar' of free movement is flanked by those of availability and accessibility of (personal and non-personal) data, which are perceived as essential values for the proper functioning of the market. Moreover, while it is true that data can sometimes be considered as a resource capable of producing pecuniary benefits[74], it is also true that certain categories of data, by reason of the purposes for which their secondary use is promoted, tend increasingly to acquire social value and utility, as a resource for enhancing the wellbeing of the community through the development of research and the improvement of policies and services.[75] In the case of health data, the value of availability is pre-eminent over the other profiles of circulation and (presumed) marketability, which, on the other hand, seem to characterise much more the non-particular categories of personal data[76].

In this perspective, the role of supervisory authorities and their cooperation will be increasingly essential to ensure a balanced coexistence between the multiple

72 On this point see European Commission, *Assessment of the EU Member States' rules on health data in the light of GDPR*, cit., p. 113. In literature see Ballantyne, A.: "How should we think about clinical data ownership?", *J. Med. Ethics*, 2020, 46, p. 289 ff.; for a critique of the application of the paradigms of ownership and property rights to personal data, see Viterbo, F.G.: *Protezione dei dati personali e autonomia negoziale*, cit., p. 145 ff.

73 For the definition of these entities, see Article 2, nn. 8) and 9) of the Data Governance Act.

74 This aspect emerges from the following definition of 'data sharing' under Article 2, n. 10) of the Data Governance Act: 'the provision of data by a data subject or a data holder to a data user for the purpose of the joint or individual use of such data, based on voluntary agreements or Union or national law, directly or through an intermediary, for example under open or commercial licences subject to a fee or free of charge'.

75 Camardi, C.: "Sulla governance digitale europea: una proposta di confronto", *Accademia*, 2023, p. 9.

76 For the main bibliographical references on the issue of the commercial value of personal data see back, footnote 1. In this regard, however, we agree with those who observe that, from the point of view of constitutional personalism, the use of data cannot be justified in a mercantile logic, in a buying and selling of them disguised by a surreptitious use of them as payment for a service, beyond the apparent gratuitousness: Perlingieri, P.: "Note sul «potenziamento cognitivo»", *Tecn. Dir.*, 2021, p. 215 s.

functions that can be ascribed to data spaces or ecosystems, on the basis of appropriate controls and interventions operating on at least three different levels: legal, technical-scientific and ethical-social.[77] It must always be borne in mind that not everything that is technically possible is in itself ethically or legally acceptable[78].

To sum up, the greatest risk to be avoided for the future is that the current European human-centric approach to the problems of personal data circulation will fade the colouring of its principles to give way to the darker hues and chiaroscuros of the state-centric and market-centric approaches to the new challenges posed by the demands of data availability and marketability[79].

77 See Zoppini, A.: "Il ruolo e le funzioni delle authorities nel trattamento algoritmico dei dati", in P. Perlingieri et al. (eds.), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, cit., p. 291 ff.

78 In this regard see Perlingieri, P.: "Note sul «potenziamento cognitivo»", cit., p. 209 ff.

79 In line with the above-mentioned wish, the European Commission, in its aforementioned Communication on 'A European Strategy for Data', outlines, in paragraph 2, the following overall situation: 'competitors such as China and the US are already innovating quickly and projecting their concepts of data access and use across the globe. In the US, the organisation of the data space is left to the private sector, with considerable concentration effects. China has a combination of government surveillance with a strong control of Big Tech companies over massive amounts of data without sufficient safeguards for individuals […] we have to find our European way, balancing the flow and wide use of data, while preserving high privacy, security, safety and ethical standards. […] The Commission's vision stems from European values and fundamental rights and the conviction that the human being is and should remain at the centre'. It must be added, however, that legislating is not enough for this purpose. A fundamental instrument is the dissemination of an anthropocentric and solidarity-based culture supported by adequate education: Perlingieri, P.: "Sul trattamento algoritmico dei dati", cit., p. 190.

BIBLIOGRAPHY

Agnino, F.: "Nozione di dati genetici ed il decalogo di legittimità al loro trattamento", *Danno e resp.*, 2014, p. 43 ff.

Amram, D.: "Building up the "Accountable Ulysses" model. The impact of GDPR and national implementations, ethics, and health-data research: Comparative remarks", *Computer Law & Security Review*, 37, 2020, p. 1 ff.

Amram, D.: "The Role of the GDPR in Designing the European Strategy on Artificial Intelligence: Law-Making Potentialities of a Recurrent Synecdoche", *Opinio Juris in Comp.*, 1, 2020, p. 1 ff.

Ballantyne, A.: "How should we think about clinical data ownership?", *J. Med. Ethics*, 2020, 46, p. 289 ff.

Bartow, A.: "Our Data, Ourselves: Privacy, Propertization, and Gender", *University of San Francisco Law Review*, 2000, p. 634 ff.

Becker, R., Comandé, G. et Al.: "Secondary Use of Personal Health Data: When Is It "Further Processing" Under the GDPR, and What Are the Implications for Data Controllers?", *Eur. J. Health Law*, 2022, p. 1 ff.

Bravo, F.: "Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act", *Contr. impr./Eur.*, 2021, p. 199 ff.

Bygrave, L.A.: *Data Protection Law. Approaching its Rationale, Logic and Limits*, L'Aia, 2002, p. 120 ff.

Bygrave, L.A., Tosoni, L.: "Article 4(15). Data concerning health", in C. Kuner, L.A. Bygrave, C. Docksey, (eds), *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford, 2020, p. 217 ff.

Bygrave, L.A., Tosoni, L., "Article 4(13). Genetic data", in C. Kuner, L.A. Bygrave, C. Docksey, (eds), *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford, 2020, p. 196 ff.

Bygrave, L.A.: "Art. 22 Automated individual decision-making, including profiling", in C. Kuner, L.A. Bygrave, C. Docksey, (eds), *The EU General Data Protection Regulation. A Commentary*, Oxford, 2020, p. 539 ff.

Cabrio, A.: "La seconda vita dei dati. Luci e ombre della normativa privacy in materia di secondary data use", in F. Frattino, F. Massimino (eds.), *I dati. Il futuro della sanità. Strumenti per una reale innovazione*, Milan, 2022, p. 25 ff.

Caggia F.: "Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario", in V. Cuffaro, R. D'Orazio, V. Ricciuto (eds.), *Il codice del trattamento di dati personali*, Turin, 2007, p. 405 ff.

Califano, L.: "Fascicolo sanitario elettronico (Fse) e dossier sanitario: il contributo del Garante privacy al bilanciamento tra diritto alla salute e diritto alla protezione dei dati personali", *Sanità pubblica* e *privata*, 2015, 3, p. 7 ff.

Calzada, I.: "Citizens' Data Privacy in China: The State-of-the-Art of the Personal Information Protection Law (PIPL)", *Smart Citi*es, 2022, 5, p. 1129 ff.

Camardi, C.: "Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali", *Giust. civ.*, 2019, p. 499 ff.

Camardi, C.: "Sulla governance digitale europea: una proposta di confronto", *Accademia*, 2023, p. 2 ff.

Cate, F.H. Dempsey, J.X. and Rubinstein, I.S.: "Systematic government access to private-sector data", *International Data Privacy Law*, 2012, p. 195 ff.

Cerea, F.: "Intelligenza artificiale a servizio dei pazienti per il contrasto a CoViD-19", *Nuova Giur. Comm.*, 2020, suppl., p. 45 ff.

Cerrina Feroni, G.: "Luci e ombre della Data Strategy europea", 13 maggio 2022, in *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9769786*

Ciancimino, M.: *Protezione* e *controllo dei dati in ambito sanitario* e *intelligenza artificial*e, Naples, 2020.

Ciatti, A.: "La protezione dei dati idonei a rivelare lo stato di salute nella legge n. 675 del '96", *Contr. impr./Eur.*, 1998, p. 368 ff.

Clifford, D. Graef, I. Valcke, P.: "Pre-formulated Declarations of Data Subject Consent - Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections", *German Law Journal*, 2019, p. 679 ff.

Comandé, G.: "Leggibilità algoritmica e consenso al trattamento dei dati personali, note a margine di recenti provvedimenti sui dati personali", *Danno resp.*, 2022, p. 141 ff.

Comandé, G., Nocco, L., Peigné, V., "Il fascicolo sanitario elettronico: uno studio multidisciplinare", *Riv. it. med. leg.*, 2012, 105 ff.

Corti, D.: "La sorte (incerta) della ricerca sui campioni biologici umani all'indomani della decisione Shardna", *Nuova giur. civ. comm.*, 2022, p. 594 ff.

Courbier, S., Dimond, R., Bros-Facer, V.: "Share and protect our health data: an evidence based approach to rare disease patients' perspectives on data sharing and data protection - quantitative survey and recommendations", *Orphanet Journal of Rare Diseases*, 2019, p. 175 ff.

D'Acquisto, G., Naldi, M.: *Big Data e privacy by design. Anonimizzazione Pseudonimizzazione Sicurezza*, Turin, 2017.

De Franceschi, A.: "Il «pagamento» mediante dati personali", in Ricciuto, V., Cuffaro V., D'Orazio R. (eds.), *I dati personali nel diritto europeo*, Torino, 2019, p. 1381 ff.

Di Ciommo, F.: "La privacy sanitaria", in R. Pardlesi (ed.), *Diritto alla riservatezza e circolazione dei dati personali*, Milan, 2003, p. 239 ff.

Dierks, C., Kircher, P., Husemann, C., Kleinschmidt, J., and Haase, M.: *Data Privacy in European Medical Research: A Contemporary Legal Opinion*, Berlin, 2021.

Drinhausen, K. Brussee, V.: "China's Social Credit System in 2021: From fragmentation towards integration", 2021, available at *https://merics.org/en/report/chinas-social-credit-system-2021-fragmentation-towards-integration*

Ducato, R.: "Data protection, scientific research, and the role of information", *Computer Law & Security Rev.*, 2020, p. 2 ff.

Federico, A.: "Applicazione dei princípi generali e funzione nomofilattica", *Rass. dir. civ.*, 2018, p. 820 ff.

Femia, P.: "Tre livelli di (in)distinzione tra princípi e clausole generali", in G. Perlingieri, M. D'Ambrosio (ed.), *Fonti, metodo e interpretazione*, Napoli, 2017, p. 209 ff.

Ferola, L.: "Le 'misure di garanzia' a tutela dei dati biometrici, genetici e sulla salute", in Pizzetti, F.(ed.): *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, Turin, 2021, p. 411 ff.

Finocchiaro, G.: "Il quadro di insieme sul Regolamento europeo sulla protezione dei dati personali", in Ead. (ed.), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, p. 2 ff.

FINOCCHIARO, G.: "Il trattamento dei dati sanitari: alcune riflessioni critiche a dieci anni dall'entrata in vigore del Codice in materia di protezione dei dati personali", in G.F. FERRARI (ed.), *La legge sulla privacy dieci anni dopo*, Milan, 2008, p. 207 ff.

FLORIDI, L.: *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milan, 2017.

GAMBINO, A.: "Dignità umana e mercato digitale", in G. CONTALDI (ed.), *Il mercato unico digitale*, Rome, 2017, p. 7 ff.

GAMBINO, A.: "Riforma del fascicolo sanitario elettronico nell'emergenza sanitaria", in C. PETRINI, C. D'APRILE, G. FLORIDIA, S. GAINOTTI, L. RIVA, S. TAMIOZZO (eds.), *Tutela della salute individuale e collettiva: temi etico-giuridici e opportunità per la sanità pubblica dopo COVID-19*, Roma, 2020, p. 36 ff.

GAMBINO, A., MAGGIO, E., OCCORSIO, V.: "Il nuovo fascicolo sanitario elettronico: sottoscrizione, tutela dei dati, responsabilità civile", 22 luglio 2020 *(https://www.dimt.it/la-rivista/articoli/nuovo-fascicolo-sanitario-elettronico/)*

GERARDS, J.H.: "General Issues concerning Genetic Information", in ID., A.W. HERINGA, H.L. JANSSEN (eds), *Genetic Discrimination and Genetic Privacy in a Comparative Perspective*, Oxford, 2005, p. 5 ff.

GEROGIEVA, L., KUNER, C.: "Article 9. Processing of special categories of personal data", in ID., L.A. BYGRAVE, C. DOCKSEY, (eds), *The EU General Data Protection Regulation. A Commentary*, Oxford, 2020, p. 372 ff.

GUARDA, P.: "I dati sanitari", in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (eds.), *I dati personali nel diritto europeo*, Torino, 2019, p. 591 ff.

GUARDA, P.: *Fascicolo sanitario elettronico e protezione dei dati personali*, Trento, 2011.

HACKER, P., "Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law", *Common Market Law Review*, 2018, p. 1143 ff.

IRTI, C.: *Consenso "negoziato" e circolazione dei dati personali*, Turin, 2021.

IRTI, C.: "L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano", *Persona e mercato*, 2023, p. 32 ff.

Kostka, G.: "China's social credit systems and public opinion: Explaining high levels of approval", *New Media & Society*, 2019, p. 1565 ff.

Lattanzi, R.: "Ricerca genetica e protezione dei dati personali", in Aa.Vv., *Il governo del corpo*, I, in P. Zatti, S. Rodotà (eds.), *Trattato di biodiritto*, Milano, 2011, p. 319 ff.

Laurie, G.: *Genetic Privacy: A Challenge to Medico-Legal Norms*, Cambridge, 2002.

Lessig, L.: "Privacy as Property", *Social Research*, 2002, p. 247 ff.

Liang, F. Das, V. Kostyuk, N. Hussain, M.: "Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure", *Policy & Internet*, 2018, p. 415 ff.

Litman, J.: "Information Privacy/Information Property", *Stanford Law Review*, 2000, p. 1283 ff.

Mac Síthigh, D. Siems, M.: "The Chinese social credit system: a model for other countries?", *Modern Law Review*, 2019, p. 1034 ff.

Malgieri, G.: "Data protection and research: A vita challenge in the era of Covid-19 pandemic", *Computer Law & Security Rev.*, 2020, p. 1 ff.

Marelli, L., Lievevrouw, E., Van Hoyweghen I.: "Fit for purpose? The GDPR and the governance of European digital health", *Policy Studies*, 2020, p. 447 ff.

Maschio F.: "Il trattamento dei dati sanitari. Regole generali e particolari del trattamento per finalità di rilevante interesse pubblico", in G. Santaniello (ed.), *La protezione dei dati personali*, in Id. (dir.), *Trattato di diritto amministrativo*, XXXVI, Padova, 2005, p. 485 ff.

Mayer-Schönberger, V., Ingelsson, E., "Big Data and Medicine - a Big Deal?", *Journal of Internal Medicine*, 2018, p. 283 ff.

Modafferi, F.: "Il regime particolare dei trattamenti dati effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri", in F. Pizzetti (ed.), *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, Turin, 2021, p. 397 ff.

Nissenbaum, H.: "A Contextual Approach to Privacy Online", *Daedalus*, 2011, p. 140 ff.

Noce, S., Ottaviano, M.: "Medicina d'iniziativa, come renderla compliant al GDPR", 18 May 2022, available at *https://www.agendadigitale.eu/sicurezza/medicina-diniziativa-come-renderla-compliant-al-gdpr/*

Noto La Diega, G.: "Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information", *JIPITEC*, 2018, 9, p. 1 ff.

Orviský, M., Klátik, J.: "Telemedicine as a part of globalization and tool for innovation from the legal point of view", *SHS Web of Conf.*, 92, 2021, p. 6 ff.

Perlingieri, C.: "eHealth and Data", in R. Senigaglia, C. Irti, A. Bernes (eds.), *Privacy and Data Protection in Software Services*, Springer ed., 2021, p. 127 ff.

Perlingieri, C.: "Coronavirus e tracciamento tecnologico: alcune riflessioni sull'applicazione e sui relativi sistemi di interoperabilità dei dispositivi", *Actual. iur. iberoam.*, 2020, p. 836 ff.

Perlingieri, C.: "Responsabilità civile e robotica medica", *Tecn. Dir.*, 2020, p. 161 ff.

Perlingieri, P.: "Privacy digitale e protezione dei dati personali tra persona e mercato", *Foro napoletano*, 2-2018, p. 481 ff.

Perlingieri, P.: "Sul trattamento algoritmico dei dati", *Tecn. Dir.*, 2020, p. 181 ff.

Perligieri, P. and Femia, P.: *Nozioni introduttive e principi fondamentali del diritto civile*, Napoli, 2000.

Perlingieri, P.: "Note sul «potenziamento cognitivo»", *Tecn. Dir.*, 2021, p. 209 ff.

Piria, C.A., "Aspetti contrattuali delle sperimentazioni cliniche no-profit", *Contratti*, 2022, p. 346 ff.

Pizzetti, F.: "GDPR, Codice novellato e Garante nell'epoca dei Big Data e dell'Intelligenza Artificiale", in Id. (ed.), *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, Turin, 2021, p. 234 ff.

Pizzetti, F.: "La protezione dei dati personali e la sfida dell'Intelligenza Artificiale", in Id. (ed.), *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Turin, 2018, p. 5 ff.

Poullet, Y.: "Data Protection Between Property and Liberties. A Civil Law Approach", in H.W.K. Kaspersen, A. Oskamp eds, *Amongst Friends in Computers and*

Law. A Collection of Essays in Remembrance of Guy Vandenberghe, The Hague, 1990, p. 160 ff.

Price, W.N., Cohen, I.G.: "Privacy in the Age of Medical Big Data", *Nature Medicine*, 2019, p. 25 ff.

Purtova, N.: *Property Rights in Personal Data: a European perspective*, L'Aia, 2011.

Rauccio, C.: "Artificial intelligence and genomics: the Data protection implications in the use of AI for genomic diagnostics", *Eur. J. Privacy Law Tech.*, 2021, p. 115 ff.

Resta, G.: "Biobanche, ricerca scientifica e tutela della persona", in P. Perlingieri et al. (eds.), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, Napoli, 2020, p. 41 ff.

Ricciuto, V.: "Circolazione e scambio dei dati personali. Il problema della regolazione del nuovo fenomeno patrimoniale", *Riv. dir. impr.*, 2021, p. 261 ff.

Ricciuto, V.: "La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno", in Id., Cuffaro V., D'Orazio R. (eds.), *I dati personali nel diritto europeo*, Torino, 2019, p. 23 ff.

Ricciuto, V.: *L'equivoco della privacy. Persona vs. dato personale*, Naples, 2022.

Rodotà, S.: "Tra diritto e società. Informazioni genetiche e tecniche di tutela", *Riv. crit. dir. priv.*, 2000, p. 596 ff.

Schwartz, P.M.: "Property, Privacy and Personal Data", *Harvard Law Review*, 2004, p. 2056 ff.

Sica, S. and D'Antonio, V.: "La commodification dei dati personali nella data driven society", in Stanzione, P.: "Introduzione", in Id. (ed.): *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Turin, 2022, p. 129 ff.

Sirgiovanni, B.: "Informed Consent to Processing of Genetic Data", *ItaLJ*, 2022, p. 955 ff.

Spatuzzi, A.: "Contratto di fornitura di servizi digitali e ruolo del consenso al trattamento dei dati personali", *Notariato*, 2021, p. 371 ff.

Stanzione, P.: "Introduzione", in Id. (ed.): *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Turin, 2022, p. 1 ff.;

THOBANI, S.: "Il pagamento mediante dati personali", in S. ORLANDO, G. CAPALDO (eds.), *Annuario 2021 Osservatorio Giuridico sulla Innovazione Digitale*, Roma, 2021, p. 361 ff.

UBERTAZZI, L.C.: "Banche dati e privacy", *Diritto industriale*, 2002, p. 633 ff.

UDA, G.M.,: "Il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricercar scientifica o storica o a fini statistici", in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (eds.), *I dati personali nel diritto europeo*, Torino, 2019, p. 569 ff.

VERSACI, G.: "Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection", *Eur. Rev. C. L.*, 2018, p. 374 ff.

VIMERCATI, F.: "Intelligenza artificiale in sanità", in P. PERLINGIERI, S. GIOVA e I. PRISCO (eds.), *Rapporti civilistici e intelligenze artificiali: attività e responsabilità*, Naples, 2020, p. 211 ff.

VIRZÌ, A., ET AL., "Comprehensive Review of 3D Segmentation Software Tools for MRI Usable for Pelvic Surgery Planning", *Journal of Digital Imaging*, 2020, p. 99 ff.

VITERBO, F.G.: *Protezione dei dati personali e autonomia negoziale*, Naples, 2008

VITERBO, F.G.: "Freedom of contract and the commercial value of personal data", *Contratto e impresa/Europa*, 2-2016, pp. 593 ff.

VITERBO, F.G.: "The 'User-Centric' and 'Tailor-Made' Approach of the GDPR Through the Principles It Lays down", *Italian Law Journal*, 2-2019, pp. 631 ff.

VIVARELLI, A.: "La tutela dei dati «sensibili» al vaglio delle Sezioni Unite", *ibid.*, p. 278 ff.

WIESE SVANBERG, C.: "Art. 89. Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes", in C. KUNER, L.A. BYGRAVE, C. DOCKSEY, (eds), *The EU General Data Protection Regulation. A Commentary*, Oxford, 2020, p. 1240 ff.

ZARSKY, T.Z.: "Incompatible: The GDPR in the Age of Big Data", *Seton Hall Law Review*, 2017, p. 47 ff.

ZENO ZENCOVICH, V.: "Profili negoziali degli attributi della personalità", *Dir. inf.*, 1993, p. 547 ff.

ZITTRAIN, J.: "What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication", *Stanford Law Rev.*, 2000, p. 1201 ff.

ZOPPINI, A.: "Il ruolo e le funzioni delle authorities nel trattamento algoritmico dei dati", in P. PERLINGIERI ET AL. (eds.), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, Napoli, 2020, p. 291 ff.

ZUIDERVEEN BORGESIUS, F.J.: "Strengthening legal protection against discrimination by algorithms and artificial intelligence", *The International Journal of Human Rights*, 2020.