Chapter 1 Introduction

1.1 General introductory remarks

The diffusion of digital technologies has a significant social and economic impact on societies[1]. Information technology provides great opportunities for individuals and communities in many domains[2].

In 2019, a qualitative study by the Organisation for Economic Cooperation and Development (OECD) examined how digital transformation affects human well-being[3]. Starting in the 1990s, the digital revolution has deeply transformed health, education, work-life balance, housing, social connections, governance, etc. The OECD's Report assesses these impacts by analysing pivotal and context-dependent opportunities and risks. One of the 11 specified "key dimensions" of people's well-being is *health*.

The digital age has especially revolutionised the healthcare delivery system and industry[4]. The term *e-health* identifies the use of information tech-

---

1 *See* the impact of the digital age on rights, freedoms and societies in Massimo Durante. *Potere computazionale. L'impatto delle ICT su diritto, società, sapere*. Meltemi Press, 2019. ISBN: 9788855190558; Stefano Rodotà. *Il diritto di avere diritti*. Gius. Laterza & Figli Spa, 2012. ISBN: 9788842096085; Stefano Rodotà and Paolo Conti. *Intervista su privacy e libertà*. GLF Editori Laterza, 2005. ISBN: 9788842076414; Stefano Rodotà. "Diritto, scienza, tecnologia: modelli e scelte di regolamentazione". In: *Rivista critica del diritto privato* 3 (2004), pp. 357–376. *See* also Giovanni Pascuzzi. *Il diritto dell'era digitale*. Il Mulino, Bologna, 2020. ISBN: 9788815290328; Fernanda Faini. *Data society. Governo dei dati e tutela dei diritti nell'era digitale*. Giuffrè Francis Lefebvre, 2019. ISBN: 9788828811947; Antonello Soro. *Persone in rete*. Fazi Editore, 2018. ISBN: 9788893254359; Tommaso Edoardo Frosini et al. *Diritti e libertà in Internet*. Le Monnier Università, 2017. ISBN: 9788800746502; Luciano Floridi. *The fourth revolution: How the infosphere is reshaping human reality*. Oxford: Oxford University Press, 2014. ISBN: 9780199606726.

2 *See* Giovanni Sartor. "Human rights and information technologies". In: *The Oxford handbook of law, regulation and technology*. Oxford University Press, 2017, pp. 424–450, p. 425. According to Sartor, information technology contributes to economic development, culture and education, art and science, public administration and communication, etc.

3 *See* OECD. *How's Life in the Digital Age? Opportunities and Risks of the Digital Transformation for People's Well-being*. 2019.

4 *See* Jelena Madir. *Healthtech. Law and Regulation*. Elgar Commercial Law and Practice, 2020. ISBN: 9781839104893.

nology for collecting and managing data related to health[5]. New digital technologies affect healthcare provision and improve the effectiveness and efficiency of health systems[6].

The positive impact of e-health technologies has been recognised at a national and international level[7]. On 26 May 2018 the World Health Assembly approved the Resolution on Digital Health, which highlights the potential of digital technologies to support health promotion and disease prevention by improving the accessibility, quality and affordability of health services[8]. However, it is difficult to gauge the concrete outcomes and multiple risks that arise with these opportunities.

Although digitisation has the potential to improve patient experiences and healthcare delivery, the increased production and advanced use of medical data open new scenarios that may expose people to high privacy risks[9]. Concerns about privacy, data protection and security of e-health technologies have been expressed by academic scholars[10], institutions, governments and public opinion[11]. Similarly, the WHO Assembly urges

---

5 *See* e.g. William W. Lowrance. *Privacy, confidentiality, and health research*. Vol. 20. Cambridge University Press, 2012. ISBN: 9781139107969.

6 *See* OECD, *How's Life in the Digital Age? Opportunities and Risks of the Digital Transformation for People's Well-being*. *See* further Chapter 3, Section 3.2.

7 *See* Walter Ricciardi. "Assessing the impact of digital transformation of health services: Opinion by the Expert Panel on Effective Ways of Investing in Health (EXPH)". In: *European Journal of Public Health* 29. Supplement 4 (2019), ckz185–769.

8 World Health Organisation (WHO), Resolution WHA71.7 on Digital Health of 26 May 2018. Retrieved from: <apps.who.int/gb/ebwha/pdf_files/WHA71/A71_R7-en.pdf?ua=1>. Last Accessed on 06/10/2021.

9 *See* OECD, *How's Life in the Digital Age? Opportunities and Risks of the Digital Transformation for People's Well-being*, pp. 22, 59–66. Potential discrimination of employees and insurances' speculations are other examples of risks.

10 *See* e.g. Lowrance, *Privacy, confidentiality, and health research*; Isabell Büschel et al. "Protecting human health and security in digital Europe: how to deal with the "privacy paradox"?" In: *Science and engineering ethics* 20.3 (2014), pp. 639–658; Samantha Adams, Nadezhda Purtova, and Ronald Leenes. *Under observation: The interplay between eHealth and surveillance*. Springer, 2017. ISBN: 9783319483429; Giuseppe Aceto, Valerio Persico, and Antonio Pescapé. "The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges". In: *Journal of Network and Computer Applications* 107 (2018), pp. 125–154; Ziawasch Abedjan et al. "Data science in healthcare: Benefits, challenges and opportunities". In: *Data Science for Healthcare*. Springer, 2019, pp. 3–38. ISBN: 9783030052492.

11 *See ex multis* OECD. *OECD Recommendation on Health Data Governance*. 2017; Council of the European Union, EU Council. *Council conclusions on Health*

WHO Member States to develop more data protection policies for mitigating such risks[12].

The importance of ensuring the right to privacy and to data protection has grown in the digital age[13]. Technologies are often designed in a way that maximises the collection and the processing of personal data. The term "personal data" in the European Union is defined by Article 4 of the General Data Protection Regulation (GDPR)[14] as follows:

> "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an

---

in the Digital Society — making progress in data-driven innovation in the field of health. Council conclusions 52017XG1221(01). Brussels, Belgium: Council of the European Union, Dec. 21, 2017; P. Arak and A. Wójcik. *Transforming eHealth into a political and economic advantage*. Polityka Insight, 2017; Francisco Lupiáñez-Villanueva et al. *Benchmarking Deployment of eHealth Among General Practitioners*. Luxembourg: Publications Office of the European Union. 2018.

12 *See* the Report by WHO, *supra* note 8, point n. 10, p. 3.

13 As regards the terminological difference, see Chapter 2, Section 2.2. On why privacy matters *see ex multis* the analysis by Daniel J. Solove. "The Myth of the Privacy Paradox". In: *Geo. Wash. L. Rev.* 89 (2021), pp. 1–51.

14 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). O.J. L. 119, 4.5.2016. Generally, on the GDPR *see* Franco Pizzetti. *Privacy e il diritto europeo alla protezione dei dati personali: Dalla Direttiva 95/46 al nuovo Regolamento europeo*. G. Giappichelli Editore, 2016. ISBN: 9788892104501; Luca Bolognini, Enrico Pelino, and Camilla Bistolfi. *Il regolamento privacy europeo: commentario alla nuova disciplina europea sulla protezione dei dati, in vigore da maggio 2016*. Giuffrè Editore, 2016. ISBN: 9788814166594; Paul Voigt and Axel Von dem Bussche. *The EU General Data Protection Regulation (GDPR). A Practical Guide*. Cham: Springer International Publishing, 2017. ISBN: 9783319579580; Giusella Finocchiaro. *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*. Zanichelli, Torino, 2017. ISBN: 9788808521057; Vincenzo Cuffaro, Roberto D'Orazio, and Vincenzo Ricciuto. *I dati personali nel diritto europeo*. G. Giappichelli Editore, Torino, 2019. ISBN: 9788892112742; Rocco Panetta. *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato D.lgs. n. 196/2003 (Codice Privacy)*. Giuffrè Francis Lefebvre, 2019. ISBN: 9788828809692; Christopher Kuner et al. *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020. ISBN: 9780198826491; Indra Spiecker gen. Döhmann et al. *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020. ISBN: 9780198826491; Bart Van der Sloot. *The General Data Protection Regulation in Plain Language*. Amsterdam University Press, 2020. ISBN: 9789048553594.

> identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Instead, "personal information" is the predominant expression used in the US legal framework[15]. Decisions on the technological design affect individuals and their personal data or personal information in increasingly pervasive ways[16].

Generally, every design regulates its medium. In this study, the term *design* refers to the set of rules, procedures and activities that plan and define an Information and Communication Technology (hereinafter: ICT). From an engineering point of view, the International Standard ISO/IEC/IEEE 15288:2015(E) on "System and software engineering – System life cycle processes" defines "design" as the "process to define the architecture, systems elements, interfaces, and other characteristics of a system or system element"[17]. According to this standard, design is also the result of the process that includes all the information and specification of attributes and systems elements. However, in the present study the term is also used to indicate the organisational procedures and measures.

Design choices shape the interaction between users, as consumers or costumers, and the products and services they buy, or they have access to. Thus, how the technology is designed inevitably affects people. Hartzog investigated the impact of design choices on individual privacy in his book *Privacy's blueprint*[18]. As Hartzog noted, designers and engineers are choice

---

15 On this topic, *see* Christopher Anglim, Jane E. Kirtley, and Gretchen Nobahar. *Privacy Rights in the Digital Age*. Grey House Publishing, 2016. ISBN: 9781642650778. On the notion of "personal data" or information *see* Chiara Angiolini. *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*. G. Giappichelli Editore, 2020. ISBN: 9788892134362; Lee A. Bygrave and Luca Tosoni. "Chapter I General principles (Articles 1–4). Article 4(1). Personal Data". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 103–114. ISBN: 9780198826491.

16 *See* the prominent analysis by Woodrow Hartzog. *Privacy's blueprint: the battle to control the design of new technologies*. Harvard University Press, 2018. ISBN: 9780674976009.

17 *See* ISO. *ISO/IEC/IEEE International Standard-Systems and software engineering – System life cycle processes*. Tech. rep. ISO/IEC/IEEE 15288 First edition 2015–05–15, 2015.

18 Hartzog, *Privacy's blueprint: the battle to control the design of new technologies*. The author elaborated a blueprint for privacy defining a framework for law and policy.

architects[19]. When designing and developing ICTs, they determine how personal data are collected and processed in the hardware or software. According to the same scholar, technology shapes consumers' choices and behaviour for the following reasons[20]: privacy-relevant design is embedded in every action and operation (e.g. when creating an online account); design is power since it can impose an order and people are easily malleable; design is not neutral, but political.

Hence, design plays a central role and has a considerable impact on personal data. It can be argued that technical design represents a tool for enforcing a defined set of rules. Rules and constraints could be settled and imposed by the market, the law and the architecture of the code[21]. Legal rules can be prescribed by regulations, statutes, or principles. The regulatory framework on data protection and its principles define the rules for data processing. This set represents the protection *by regulation*. Conversely, the code regulates *by design*.

The present study attempts to show that the interaction between *law* and *design* could address some data protection issues in the existing legal framework of the European Union (EU) and in particular in the e-health sector. Fundamental for this purpose is the proactive approach called *privacy by design*, which aims to address data protection concerns by embedding legal requirements in the ICT's design.

Privacy by design (hereinafter also: PbD) is a major concept of interest within the field of privacy and data protection law[22]. Its main goal is to design a system, product or service in a way that "supports and applies" privacy principles and legal provisions[23]. It is important to note that technical and organisational strategies are both essential for PbD. Though so far high importance has been assigned to the technological aspects, admin-

19 Hartzog, *op. cit.*, p. 35.

20 Hartzog, *op. cit.*, pp. 21–55.

21 *See* the work of Lawrence Lessig. *Code and other Laws of Cyberspace*. 1999. ISBN: 9780465039128; Lawrence Lessig. *Code*. 2.0. New York: Basic Books, 2006. ISBN: 0465039146. *See* further Chapter 2, Section 2.2.

22 As will be presented later, PbD was first conceptualised by a Canadian Privacy Commissioner and was later recognised as an international principle for protecting privacy.

23 *See* the definition reported in Giorgia Bincoletto. "A Data Protection by Design Model for Privacy Management in Electronic Health Records". In: *Privacy Technologies and Policy, 7th Annual Privacy Forum, APF 2019, Rome, Italy, June 13–14, 2019*. Ed. by Maurizio Naldi et al. Lecture Notes in Computer Science. Springer International Publishing, 2019, pp. 161–181. ISBN: 9783030217525.

istrative and bureaucratic solutions are also fundamental for mitigating privacy and data protection risks.

Technical and organisational measures are combined in the General Data Protection Regulation. Article 25 establishes the binding obligations of *data protection by design* (from now on also: DPbD) and *data protection by default* (from now on also: DPbDf). As will be discussed in Chapter 2, privacy by design and data protection by design should be considered different concepts. Given this premise, the former will be the starting point of the discussion, while the latter will be central to the entire work.

Although extensive research has been carried out on PbD, there are few studies that have investigated in a systematic way the interactions between DPbD obligation and the healthcare context. Thus, this book examines how an e-health system in the EU could be developed and data processing carried out in a way that supports data protection principles, rules and requirements by design in order to better protect personal health data. This study investigates the significance of the data protection by design obligation in the e-health care sector by taking into account the legal framework of the EU.

As mentioned, the latest improvements in the e-health care field have led to new privacy and data protection issues. Personal health data represent sensitive information concerning a data subject and require a higher level of protection since they have been recognised in the particular category of personal data[24]. Therefore, enhancing data protection and security of e-health systems has become a primary interest in the EU[25].

E-health is an important component of the EU agenda. Although jurisdiction over health matters remains in the hands of Member States[26], health policies have been developed and promoted by EU institutions[27].

---

24 *See* further Chapter 3, Section 3.3.1.

25 *See* EC European Commission. "eHealth Action Plan 2012–2020. Innovative healthcare for the 21st century". In: *Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions. Brussels, 6.12. 2012* (2012). The EC stated that "effective data protection is vital for building trust in eHealth".

26 The EU shares the competence with Member states on "common safety concerns in public health matters" according to Article 4(k) of the Treaty on the Functioning of the European Union and supports and coordinates Member States' action according to Article 6(a) of the same Treaty. *See* Arak and Wójcik, *Transforming eHealth into a political and economic advantage*. *See* further Chapter 3, Section 3.3.

27 One of the main areas is free access to healthcare across countries, as will be described in Chapter 3, Section 3.3.

However, the issues related to data protection are considered barriers to the adoption of e-health technologies[28].

The European Commission's eHealth Action Plan 2012–2020 stated that in the e-health context ICTs should integrate the principle of privacy by design and by default[29]. In the Digital Single Market Strategy for Europe[30], the European Commission (EC) suggested that e-health infrastructures should be built in accordance with data protection rules[31]. Since the entry into force of the GDPR, the EU has a uniform framework for data protection law[32].

In this context, the role of DPbD in protecting personal health data is a relevant subject of investigation. The issue is how to comply with a principle, approach, or obligation that requires implementing technical and organisational strategies and measures by design for safeguarding the right to data protection.

Although the EU legal regime is the main focus of this research, an examination of a comparable legal system is indispensable for the topic[33]. Looking at the US system from a comparative perspective will be of great help in understanding how technical and administrative measures are

---

28 It has been highlighted that the concerns are voiced by both patients and health professionals. *See* Lupiáñez-Villanueva et al., *Benchmarking Deployment of eHealth Among General Practitioners*.

29 European Commission, "eHealth Action Plan 2012–2020. Innovative healthcare for the 21st century".

30 *See* the official website of the Digital Single Market Strategy at <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age >. Last accessed 06/10/2021.

31 *See* EC European Commission. *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society*. European Commission. Brussels, 25.4.2018 COM (2018) 233 final, 2018, p. 5. *See* also EC European Commission. *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions A European strategy for data*. European Commission. Brussels, 19.2.2020 COM (2020) 66 final, 2020.

32 In addition to the GDPR, the EU directive 2016/1148 on the security of network and information systems (NIS Directive) concerns "measures for a high common level of security of network and information systems across the Union" and it is transposed by Member States from national laws.

33 On the comparative methods used by different disciplines *see* Giorgio Resta, Alessandro Somma, and Vincenzo Zeno Zencovich. *Comparare. Una riflessione tra le discipline*. Mimesis Edizioni, 2020. ISBN: 9788857567310.

implemented in another legal framework that provides special rules for protecting health information[34].

Moreover, in light of the title of the present book "Data protection by design in the e-health care sector: theoretical and applied perspectives", the theoretical research on DPbD is a precursor to a more in-depth study on the healthcare context, including a case study on an e-health technology, the Electronic Health Record (EHR) system.

There is currently a lack of clarity and knowledge among developers, data controllers and stakeholders on how to comply with the DPbD provisions. The overall purpose is to contribute to the line of research that bridges the gap between the legal and technical disciplines on DPbD by providing a comprehensive set of guidelines for the implementation of the principle in the case study.

The book does not engage with ethical approaches, Big Data and Artificial Intelligence (AI) concerns[35]. Moreover, it is beyond the scope of this study to examine the interactions between Big Data and the e-health sector and the secondary use of personal health data. So, a discussion of AI and privacy or data protection lies beyond the scope of this research.

---

34 The comparative approach will be further explained in Section 1.2.

35 For the definition of Big Data *see* IBM. "The 5 Vs of big data". In: *IBM Watson Health Perspectives* (2016). As regards artificial intelligence and ethical issues *see* High-Level Expert Group on AI. *Ethics Guidelines for Trustworthy Artificial Intelligence*, *AI HLEG*. European Commission, 2019; Floridi, *The fourth revolution: How the infosphere is reshaping human reality*. On the opportunities and risks of AI in the legal domain *see* Alessandro Mantelero. "Regulating AI within the Human Rights Framework: A Roadmapping Methodology". In: *European Yearbook on Human Rights*. Intersentia Ltd., 2020, pp. 477–502. ISBN: 9781780689722; Amedeo Santosuosso. *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*. Mondadori Università, 2020. ISBN: 9788861848283, Barfield Woodrow, Ugo Pagallo. *Law and artificial intelligence.* Edward Elgar Publishing. 2020. ISBN: 9781789905144. In the data protection field *see* CoE Council of Europe. *Guidelines on artificial intelligence and data protection*. Council of Europe, 2019; Giovanni Comandé. "Unfolding the legal component of trustworthy AI: a must to avoid ethics washing". In: *Annuario di Diritto Comparato e di Studi Legislativi* XI (2020), pp. 39–62; Alessandro Mantelero. "AI and Big Data: A blueprint for a human rights, social and ethical impact assessment". In: *Computer Law & Security Review* 34.4 (2018), pp. 754–772; Ira S. Rubinstein. "Big data: the end of privacy or a new beginning?" In: *International Data Privacy Law* 3.2 (2013), pp. 74–87. On PbD and these trends *see* Laura Greco and Alessandro Mantelero. "Industria 4.0, robotica e privacy-by-design". In: *Dir. informazione e informatica* 6 (2018), pp. 875–900; Alessandro Mantelero. "La privacy all'epoca dei Big Data". In: *I dati personali nel diritto europeo*. G. Giappichelli Editore, Torino, 2019, pp. 1181–1212. ISBN: 9788892112742.

The reader should bear in mind that the study is based on the interactions between DPbD and the e-health sector for processing personal health data.

1.2 Research methodology and objectives

In this subsection, a more detailed description of the research methodology and research questions are provided. The book draws on sources from law, social science, computer science and engineering.

The research can be divided between "theoretical perspective" and "applied perspective". Firstly, for the theoretical part of the research a legal and a comparative analysis is carried out. This examination is focused on PbD and DPbD by taking into account how these concepts have been elaborated by the literature, the institutions and EU data protection law. Then, a critical legal analysis on these principles is provided.

As mentioned, the research focuses on Article 25 of the GDPR. Therefore, the main perspective is EU law on data protection. However, the discussion is not always limited to that system in order to achieve an in-depth critical and comparative analysis with other perspectives. Case law is discussed where it has relevance for explaining legal concepts.

An entire chapter is dedicated to the e-health sector by investigating the data protection concerns of e-health technologies and the regulatory framework that applies. The case study of the EHR system will be analysed there by an interdisciplinary approach and by taking into account the state of the art of the technology, the applicable provisions in EU data protection law and the issues related to the data processing activities.

Moreover, a comparative law approach concentrates the study on the US framework because PbD has been recognised as an international principle in the field and there is a specific rule in the federal law of the US for e-health care, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which mandates the implementation of technical and organisational safeguards to protect health information. PbD is an international legal concept for the preventive protection of personal data, and it is based on the Fair Information Practices principles, which were first formulated in US law.

Comparative studies aim to establish similarities and differences between legal systems[36]. As scholars have highlighted, the primary purpose

36 On the methodology of comparative law *see ex multis* Rodolfo Sacco and Piercarlo Rossi. *Introduzione al diritto comparato*. Utet Giuridica, 2019. ISBN:

of comparative law as a science is to improve knowledge of each of the legal systems under scrutiny[37]. According to Zeno Zencovich, "comparing advances and deepens knowledge"[38]. The subject of investigation may be a legal rule or norm[39]. The scholar may uncover the rule by studying a "legal formant" or multiple "formants" in a legal system (i.e. statutory rule, formulation of scholars and decision of judges)[40]. It has been explained that legislative comparison aims to clearly present various solutions[41].

So, the research aims to compare Article 25 of the GDPR and the HIPAA Privacy and Security Rules that protect digital medical records.

9788859820826; Uwe Kischel. *Comparative Law*. Oxford University Press, 2019. ISBN: 9780198791355; Alessandro Somma. *Introduzione al diritto comparato*. Giappichelli, 2019. ISBN: 9788892130197; Ralf Michaels. "The Functional Method of Comparative Law". In: *The Oxford Handbook of Comparative Law*. Oxford University Press, 2019, pp. 340–382. ISBN: 9780198810230; Catherine Valcke. *Comparing law: comparative law as reconstruction of collective commitments*. Cambridge University Press, 2018. ISBN: 9781108555852; Devin Griffiths. "The comparative method and the history of the modern humanities". In: *History of Humanities* 2.2 (2017), pp. 473–505; Marieke Oderkerk. "The Need for a Methodological Framework for Comparative Legal Research: Sense and Nonsense of "Methodological Pluralism" in Comparative Law". In: *Rabels Zeitschrift für ausländisches und internationales Privatrecht/The Rabel Journal of Comparative and International Private Law* (2015), pp. 589–623; Geoffrey Samuel. *An Introduction to Comparative Law Theory and Method*. Hart Publishing, 2014. ISBN: 9781849466431; Pier Giuseppe Monateri. *Methods of Comparative Law*. Edward Elgar, 2014. ISBN: 9781781006535; Maurice Adams and Jacco Bomhoff. *Practice and Theory in Comparative Law*. Cambridge University Press, 2012. ISBN: 9780511863301; Konrad Zweigert and Hein Kötz. *Introduzione al diritto comparato*. Vol. 1. Giuffrè Editore, 2011. ISBN: 9788814155857; Pierre Legrand. *Le droit comparé*. Presses universitaires de France, 2011. ISBN: 9782130590767; Konrad Zweigert and Hein Kötz. *Introduction to comparative law*. Vol. 3. Clarendon Press Oxford, 1998.

37 *See* Sacco and Rossi, *Introduzione al diritto comparato*, p. 1; Zweigert and Kötz, *Introduzione al diritto comparato*, p. 17. A comparative legal research may also have an evaluative or regulatory objective, or it may aim to harmonise or standardise legislation in different states or nations. *See* Oderkerk, "The Need for a Methodological Framework for Comparative Legal Research: Sense and Nonsense of "Methodological Pluralism" in Comparative Law".

38 Vincenzo Zeno Zencovich. "Comparing comparative law". In: *Comparare. Una riflessione tra le discipline*. Mimesis Edizioni, 2020, pp. 227–240. ISBN: 9788857567310, p. 231.

39 Sacco and Rossi, *Introduzione al diritto comparato*, p. 11.

40 *See* Rodolfo Sacco. "Legal formants: a dynamic approach to comparative law (Installment I of II)". in: *The American Journal of Comparative Law* 39.1 (1991), pp. 1–34, p. 1.

41 *See* Zeno Zencovich, "Comparing comparative law", p. 235.

HIPAA is a sectorial regulation that protects identifiable health information by implementing organisational and technical measures. DPbD is a more general rule, but it is also applicable to personal health data and mandates the implementation of organisational and technical measures, as well. Both rules are obligations in their legal systems. The common problem is the need to better protect personal health data in a digital world by the use of safeguards. It is interesting to understand whether or not an e-health technology may be used in both the EU and the US systems. Particular attention will be given to the similarities and differences of privacy and data protection concepts and their principles (e.g. informational privacy vs. data protection, personal information vs. personal data, notice vs. privacy policy, etc.).

Secondly, in order to gain insights into e-health and to adopt an applied perspective, investigations are carried out on the existing technical solutions, engineering methodologies and approaches, and on a defined case study in the domain. Investigating for a data protection by design set of architectural and organisational guidelines for e-health systems demands an interdisciplinary approach. This method is needed in order to take into account both legal and technological concerns, identify the problems and try to find appropriate solutions[42].

Drawing on concepts and literature from law and information technology allows a wider perspective on the topic and related research issues.

Given the problems mentioned in the introductory remarks, the defined research goals and its methodologies, the research question addressed by the present book may be framed in the following way: How could an e-health system be designed, and the data processing be carried out in a way that supports and materialises data protection principles and legal requirements in order to protect personal health data?

In particular, the research work can be divided into the following subquestions and related steps:

Theoretical perspective

– What does the privacy by design legal concept indicate historically and systematically? The research focuses on this principle of *regulation by design* and investigates the PbD principle by providing a critical

42 On the interdisciplinary method *see* Giovanni Pascuzzi. *La creatività del giurista. Tecniche e strategie dell'innovazione giuridica*. Zanichelli, 2013. ISBN: 9788808164162. On problem solving *see* Giovanni Pascuzzi. *Il problem solving nelle professioni legali*. Il Mulino, Bologna, 2017. ISBN: 9788815272997.

analysis to highlight advantages and challenges of its endorsement and implementation.
- According to Article 25 of the GDPR, what does the data protection by design obligation require? The research analyses the provision in detail and other related rules of the Regulation.
- Moving into the healthcare context, what are the applicable data protection principles and rules for the protection of personal health data in the EU and, in particular, for processing operated in EHR systems? The research examines the regulatory framework that applies to the processing of personal health data and uses a case study in the e-health care sector.
- What are the results of the comparative analysis between Article 25 GDPR and the HIPAA Privacy and Security Rules by looking at the US federal legal framework? The research compares the provisions by taking into account the differences and similarities between EU and US legal systems.

Applied perspective
- What are the existing technical tools and approaches for designing data protection? What are the suitable solutions and standards for developing EHR systems? The research deals with system and software design methods, and privacy engineering approaches. It also focuses on risk assessment, privacy enhancing technologies and standards applicable to the case study.
- What comprehensive set of technical and organisational guidelines may be provided for implementing DPbD in the e-health case study of an EHR system? Finally, the book provides a set of guidelines that includes measures and safeguards for DPbD implementation to explain how system and data processing could be designed so that they incorporate data protection principles and requirements.

1.3 Structure

The book is structured as follows.

After these introductory remarks, Chapter 2 addresses the first and second points of the above mentioned sub-questions at a theoretical level. This part examines the concepts of privacy by design and data protection by design. Firstly, the Chapter presents the theoretical approach of *regulation by design* and summarises the history of privacy by design in a comparative way. Next, it conducts an extended critical analysis on the PbD

concept with special attention to striking a balance between advantages and disadvantages that may result after a legal adoption of the rule. The Chapter then focuses on Article 25 of the GDPR, which provides the data protection by design obligation, and it also deals with the related legal requirements of the GDPR. Finally, it concludes by reflecting on a comparison between PbD and DPbD concepts and balancing the right to data protection against other rights and freedoms.

The third point of the theoretical perspective is addressed by Chapter 3, which provides a legal analysis of the e-health sector and presents the case study of an Electronic Health Record system. In particular, this Chapter firstly investigates the privacy and data protection concerns that emerge from the use of digital technologies for health purposes. Then, it critically reviews the data protection law for the processing of personal health data in the EU legal framework. After these theoretical considerations, the Chapter examines the case study, including the state of the art of the technology, the applicable rules in the EU, and its cross-border use across Member States that entails interoperability issues. At the end, Chapter 3 briefly concludes with other thoughts on balancing the right to data protection against other interests, and in particular against the public interest in the healthcare domain.

Chapter 4 deals with the comparative analysis of DPbD (EU) and the HIPAA Privacy Rule (US). The Chapter starts with a brief overview of informational privacy law in the US, and reviews the privacy principles in US federal law. The goal is to investigate the similarities and differences with the data protection principles of the GDPR in light of a PbD or DPbD implementation. Later, the Chapter summarises US health privacy law and presents HIPAA Privacy and Security Rules and their requirements. Finally, it compares DPbD and HIPAA under the different frameworks since looking at the US framework may be useful for understanding how technical and administrative measures for protecting personal data are implemented in the e-health context.

Chapters 5 and 6 refer to the applied perspective. On the one hand, Chapter 5 analyses the existing technical tools, approaches and methods for designing data protection; on the other hand, Chapter 6 presents the set of guidelines for implementing DPbD in the case study. In particular, Chapter 5 deals with some general notions of system and software engineering. Then, it analyses how the field of privacy engineering has proposed approaches for applying PbD or DPbD and for assessing privacy risks. Given the e-health care sector, and the case study on EHR, the

Chapter then investigates the privacy enhancing technologies and the recognised international standards used for EHR system development.

Chapter 6 provides the set of guidelines with technical and organisational strategies and measures to be implemented in the EHRs in the European Union legal framework. The foundations of the comprehensive set of guidelines are the GDPR and the current data protection law for data concerning health in the EU, the theoretical analysis and insights discussed in Chapter 2, 3 and 4 and the applied perspective on privacy engineering presented in Chapter 5. Finally, Chapter 6 investigates some potential liability scenarios in the event of inappropriate or ineffective DPbD implementation.

Conclusions are finally presented in Chapter 7.