Chapter 7 Conclusions

7.1 Concluding remarks

The digital revolution has deeply transformed the provision of healthcare. The e-health context is one of the most data-intensive sectors and it is constantly evolving. Private and public healthcare providers are using electronic health data to ensure more effective and efficient services.

Several EU policies allocate resources to transform and enhance the protection of the right to health. E-health technologies represent both great opportunities and significant challenges. The protection of personal health data is one of the important challenges to be faced. The digital revolution has also changed the way law regulates phenomena. Law and technology should cooperate to create or apply rules in cyberspace. Since multiple processing activities occur in everyday life and in different contexts, the data protection field has become crucial in safeguarding rights and freedoms.

This research started with the concepts of *regulation by design* and *privacy by design*. *Code* creates an embedded set of rules in the technological design of ICTs and absorbs values. The design of ICTs is thus never neutral.

Technical regulation goes hand-in-hand with regulation of the market, social norms and the law. Law may interfere with the architectural constraints that are decided by developers by mandating the incorporation of legal rules in the design of technologies and related practices. It has been highlighted that law regulates *ex post*, while architecture *ex ante*. The interaction between law and design could address some legal issues in the privacy and data protection domain.

The approach of privacy by design aims to build privacy principles and requirements into the design and architecture of ICTs and organisational practices to improve legal compliance. The investigation focused on the history and philosophy that have created this principle. Starting from the research by Cavoukian, PbD proposes to minimise privacy risks and increase users' protection by following certain principles. In recent years, PbD has been promoted by authorities internationally and in some legal systems, including in the US by the FTC and in the EU framework.

An extensive critical analysis of the concept of PbD has been provided. When adopting a legal rule on PbD, or endorsing its concrete implementation, several advantages and disadvantages collide. It has been demonstrat-

ed that a provision on PbD should be framed in a detailed form with some criteria for implementation, it should be well drafted and clearly worded, and it should be neutral in order to be effective. A thorough legal analysis of all the applicable legal rules should be performed when applying PbD, but incorporating principles and requirements is a significant challenge since hard-coding law involves representing rules in a machine-readable way, interpreting legal rules, and identifying and balancing rights and interests. These complex activities are usually carried out by legal experts. As a result, these experts must be involved in the PbD implementation, which must be the result of interdisciplinary work.

PbD is a proactive, dynamic and global approach that requires concrete organisational measures, and involves investments and allocated resources, but companies sometimes lack a knowledgeable organisation and are reluctant to pay high costs. At the same time, PbD may be considered a business opportunity, a competitive advantage and a positive paradigm for increasing trust and confidence in products and services.

In the digital environment there is an information asymmetry between users and companies. This operates in knowledge and power. In the age of "surveillance capitalism", given the current economic and business models, a more effective approach to protecting personal data and privacy is necessary to challenge these dynamics and better protect rights.

PbD may be considered an innovative approach but shaping technology at the service of the law is not a trivial problem. Strategies for PbD implementation should be developed on a case-by-case basis since one solution does not fit all situations and contexts. Balancing the benefits and criticisms, PbD is an opportunity to govern new phenomena and implement privacy principles and rights. In fact, the EU chose to establish a specific "by design" provision in the GDPR.

Article 25 of the GDPR and the DPbD obligation have been investigated in detail through a legal analysis since this provision requires taking into account various criteria while implementing appropriate technical and organisational measures before and during data processing operations to safeguard principles and data subjects' rights in an effective manner. This provision is not the only requirement in the EU framework that mandates data protection by design. Other Regulations establish similar obligations to create consistency within the EU legal system and modernise all the sectors where personal data are processed.

DPbD is an enforceable obligation with which data controllers subject to the material and territorial scopes of the GDPR must comply. Even though the provision explicitly refers to the controller only, the processor

shall assist this subject in fulfilling the DPbD obligation. As regards developers of ICTs, they are not included in Article 25. However, it may be argued that they are encouraged to implement DPbD measures since controllers may select products and services on the basis of the adopted design choices.

Once again, there is no "one-size-fits-all" solution for complying with such a requirement in the whole project and during the data management life-cycle. Appropriate and effective measures must be selected according to objective (i.e. state of the art) and subjective criteria (i.e. cost of implementation, contextual factors of the data processing operations, risk assessment) for implementing data protection principles and safeguarding data subjects' rights. Several examples of measures that achieve these principles and rights have been provided, but the selection should be sector- and case-specific.

Data protection by default is another obligation mandated by Article 25. DPbDf requires the controller to implement appropriate technical and organisational measures as default settings for ensuring that the processing does not include personal data that are not necessary for the specific purpose. This provision directly entails the design of the technologies and how they automatically process personal data. The measures for implementing DPbD and DPbDf may eventually overlap, but it has been argued that the controller should have in mind both distinct principles and fulfil them by adopting a holistic "data protection first" approach. The implementation of Article 25 should also be coordinated with other rules that the GDPR sets out: security requirements, risk assessment rules and certification mechanisms upfront.

The comparison between PbD and DPbD has shown that these concepts are different, and their wording is frequently misleading. It has been pointed out that they represent broad proactive approaches. PbD is an international concept perceived as a principle and advocated by scholars and policymakers for the protection of privacy and personal data. It also includes the protection of default settings. DPbD and DPbDf are instead separately defined in Article 25 GDPR and are established for the protection of persona data. DPbD is a fully enforceable and flexible obligation, while PbD entails a visionary and ethical dimension. It is arguable that Article 25 has a broad formulation that means that it is difficult to implement, but this provision is technologically neutral, dynamic and leaves room for specific customised solutions. It is also relevant to stress that when advocating respect for DPbD, possible conditions may limit the

right to data protection, and some balancing may be necessary against other rights and freedoms.

The legal analysis moved to the healthcare context to contextualise the DPbD approach. The investigation of the data protection concerns of e-health technologies demonstrated that data concerning health deserve high protection and higher guarantees are established by the law. Data on health status can render the individual vulnerable in multiple ways. The right to respect for private life, the duties of medical and professional confidentiality, and data protection laws set a variety of rules for protecting personal health data.

The current legal framework in the EU is primarily the GDPR, but other legal sources are applicable at EU and Member States' levels. The investigation focused on this framework by providing the definition of personal health data, by discussing the legal grounds for their processing and other relevant legal requirements that apply in the context of e-health and are useful for a DPbD implementation. In particular, it has been highlighted that personal health data are included in the list of special categories of data by the GDPR because they reveal information on the health status of the data subject and merit heightened protection. The definition of this data type is broad and open to interpretation. Processing is allowed in exceptional situations where a legal ground applies. The GDPR enhanced the protection of personal health data by increasing data subjects' rights to be protected and the obligations to comply with. Special considerations have been made on the exercise of these rights and on the extent of the obligations.

The protection of personal data may be balanced against public health interests in particular scenarios, such as the recent pandemic, with additional safeguards in place. In fact, the health sector is frequently subject to national rules that derogate or further specify processing activities with legislative measures that are necessary and proportionate insofar as they respect the rights and freedoms of individuals in a democratic society.

Then a case study in the e-health domain was introduced: the EHR system. This technology is widely used for processing data concerning health at the EU level, in Member States and even across them in an interoperability scenario. The state of the art and the applicable legal framework were analysed as the EHR environment entails complex data processing operations. The description of the state of the art employed internationally recognised concepts and standards.

The EHR is a widely used technology that is considered a priority by EU policies and strategies. This system collects and processes all the personal

health data of the patient and shares them among all authorised operators that are involved in the medical treatment. From a technical point of view, several entities as source systems (i.e. healthcare providers) aggregate data in repositories in a given period of time (e.g. patient's life period), and use the whole resulting system in different ways of interaction according to multiple functions. In particular, it has been reported that the EHR is primarily used for patient care delivery and patient care management, but it is useful for patient care support processes and financial and other administrative processes since it collects both common personal data and personal health data. Three functions of the EHR were grouped: the storage with the data at rest; the network where the data are transferred; and the computation area where the data are used.

Then, the book discussed the EU legal framework applicable to the processing of data in the EHR systems. The legal analysis focused on the roles in the processing, the legitimate grounds, the necessary data protection safeguards for the national legal frameworks, and the rights and duties in the EHR environment. It also investigated the interoperability issues of the cross-border processing (and exchange) of personal health data with EHRs where data protection and security risks increase since systems are more interconnected and the amount of personal health data rises as well as the number of actors involved. It has been demonstrated that the GDPR lays down the main requirements with which healthcare providers must comply during data processing in the EHRs and that DPbD obligation must play a major role in the development of EHR systems.

Furthermore, PbD has been recognised as an international principle for the proactive protection of personal data, and is based on FIPs which were first developed in the US. In US federal law there is a specific rule for the implementation of technical and organisational measures in the e-health care context and for EHRs. Given these premises, a comparison with the US legal framework was provided by analysing the applicable principles and provisions. It may be pointed out that the protection of personal health data is actually a global issue.

The research provided an overview of information privacy law in the US and of privacy principles in US federal law. The goal was to examine the similarities and differences with the data protection principles of the GDPR in light of a PbD or DPbD implementation. In the US, informational privacy law sets the rules that protect personal information, but the framework is sectorial and fragmented. Reading the FIPs and the OECD's Guidelines it may be argued that the GDPR provides broader principles and more guarantees. Thus, the application of a PbD or a DPbD approach

might differ between the US and the EU since the implementation may follow partially different principles. Nonetheless, the core data protection or informational privacy principles are similar. It has been reported that some US scholars and the American Law Institute are proposing new formulations of the FIPs that go beyond the OECD's principles. In particular, the ALI's project is a prominent effort to reform the FIPs by including both the OECD's and GDPR's concepts in light of a modern path forward of informational privacy. However, FIPs alone are not sufficient to affect the design of technologies and business practices.

Moreover, the US legal framework for health informational privacy and for EHRs, and HIPAA Privacy and Security Rules, were analysed. These Rules establish federal standards for protecting personal health information processed by covered entities. HIPAA requires appropriate administrative, physical and technical safeguards and sets limits and conditions on use and disclosure of information.

The research compared HIPAA Privacy and Security Rules with the DPbD requirement in the e-health context. The elements of this comparative analysis were the scope of application and the rationale of the norms, the object and the recommended measures, and the underlying principles and rights. The analysis showed that, despite some interesting similarities, an EHR may not be used in both EU and US legal frameworks since the DPbD principle goes beyond a set of measures to be implemented. At the same time, HIPAA requirements can be considered useful examples of measures for developing some guidelines for the EHRs. HIPAA gives an important role to technical means for protecting privacy, but DPbD is a more global approach that guarantees further protection. An explicit legal recognition of PbD in US law may bring these frameworks together.

The research was then dedicated to a more applied perspective in the technological domain that investigates existing technical tools, approaches and methods for designing data protection. This part employed an interdisciplinary methodology.

It was pointed out that the EHR system is complex since it has a set of components that includes both hardware and software: database management systems and their hardware, EHR software with its architecture and interface, and the network. Given some general notions on systems and software engineering, it was shown that privacy or data protection needs should be formulated as requirements for system development. Despite interpretation and translation concerns, legal rules should be analysed, specific requirements or use cases should be identified and developed into functional or non-functional system requirements by following a method-

ology. Different methodologies may be adopted for software development. The choice should take into account the challenges that the selected methodology presents in connection with the DPbD implementation. In addition, the methods should consider the personal data life-cycle, which can be classified as data collection, data use and data erasure, where personal data may be at rest, in use, or in transit.

An overview of privacy engineering approaches was provided by looking at some significant contributions related to PbD and DPbD. Privacy engineering is used to design systems with privacy or data protection built into the technical design. Several approaches were defined and analysed. In general, engineering methodologies may combine the use of patterns, tactics, goals, strategies, and PETs with the definition of requirements and use cases. A methodology for DPbD implementation should take into account the GDPR's principles and requirements. In fact, engineering approaches are fundamental for a concrete implementation, but they should be combined with the applicable data protection principles and with a preventive risk analysis.

Since the risk assessment framework is crucial for Article 25 of the GDPR, the research examined the relevant concepts that are applicable to this assessment, including likelihood and severity and how they can be evaluated before the start of data processing. Moreover, this part discussed some applicable methodologies for the data protection impact assessment, which have been developed by scholars and DPAs.

After that, the research focused on the e-health care sector and the case study on EHRs, by presenting some suitable PETs and recognised international standards that are useful for EHR system implementation. All these technical insights represent tools for defining the measures to be applied in the EHR environment.

Hence, theoretical and applied perspectives of the research were combined in applying DPbD in the case study. This research tried to create a set of guidelines for DPbD implementation in EHR systems and in the EU legal framework. To provide more concrete guidance on the integration of data protection rules in the concept development phase of the EHR system and its data processing management, the comprehensive guidelines were developed by classifying both technical and organisational measures and by assigning the related data protection principles and data subjects' rights. So, the GDPR's requirements and the current data protection law for data concerning health in the EU are the foundation of this set of guidelines. The comparison with the US legal framework was also taken into account

since it provides useful examples of organisational and technical safeguards for medical records.

The set of DPbD guidelines defined requirements and comprehensive data protection measures that may aid data controllers and system developers when they make architectural choices in the requirement phase of a DPbD engineering approach, and for the appropriate organisational and technical measures to be implemented in the data processing activities. In fact, the guidelines apply to the full life cycle of data processing, i.e. before processing and during processing activities.

In the end, since the obligation to implement DPbD measures is upon data controllers, but other subjects are involved in the concrete implementation, the research provided some brief notes on liability in the event of inappropriate or ineffective DPbD implementation. It was argued that the broad discretion upon data controllers on the DPbD implementation leaves enough space for courts on ruling and on DPAs on sanctioning. In fact, the adequacy of the measures is related to an objective case-by-case evaluation of the court or the DPA, but the implementation is performed on a case-by-case basis under subjective criteria. Future DPAs' opinions or case law might provide specific guidance on the enforcement of DPbD obligation.

7.2 Open questions

Some brief open concerns may be summarised here.

First of all, it should be highlighted once again that balancing interests and rules while applying DPbD is a non-trivial problem. The tools and methodologies for integrating privacy or data protection in functional and non-functional system requirements are frequently developed without interdisciplinary approaches. So, it should be stressed that the legal and technical sides should always cooperate in defining problems and finding solutions.

Moreover, since DPbD is a global approach that requires a technical implementation by design, it may even be difficult to modify existing systems from an engineering perspective. The GDPR sets high administrative fines. So, data controllers should choose products and services in the market that indicate the DPbD implementation. This situation creates competitive concerns. Developers are out of the scope of the Regulation. Despite this, it may be argued that producers and technology developers are forced to adopt DPbD solutions to be still competitive in the market.

DPbD could set a global standard on data protection, but it should be adopted and implemented in several frameworks. Nowadays the big tech players in the "black box society" are outside the EU borders. The EU should find a way to be in the market and simultaneously lead by example in the protection of principles and rights.

In the healthcare sectors data controllers are frequently public entities. Since many technical solutions and technologies for adopting DPbD are expensive (e.g. standards), the cost of implementation criterion of Article 25 GDPR may create obstacles, or discourage implementation. However, the public sector should lead by example in effectively protecting rights and freedoms. Allocating appropriate resources for public entities and healthcare providers may enhance DPbD implementation in the e-health care sector.

Finally, specific EU certification on DPbD, codes of conduct for different sectors, including e-health, and more guidelines and opinions are needed in the future. It should be clear how courts and DPAs will rule on DPbD compliance.

7.3 Future research

In the future this research may be applied to a specific Member State or to more Member States at a comparative level to investigate how concrete EHR environments apply DPbD by following the GDPR requirements and Article 25. This will be an empirical study that uses a bottom-up approach based on existing projects of hospitals or clinics.

Alternatively, a new theoretical study may classify all the applicable rules for EHR systems or e-health technologies in general at the Member States' level to identify the residual limits for the legal and organisational interoperability in a cross-border context and to compare the rules adopted under Article 9(4) GDPR after the entry into force of the Regulation. Actually, the cross-border context remains an interesting point of research since the European Commission and eHealth Network are still working on the "Transformation of Health and Care in the Digital Single Market" and "Interoperability & standardisation: connecting eHealth services" policies.

The comparative analysis between the EU and the US may be extended to other legal frameworks. For example, Canada is an interesting legal framework to investigate since it is the country where the PbD concept was first developed, it has an active data protection authority, and the rules are established both at national and provincial levels. China is another in-

triguing legal system. Advanced e-health technologies are produced there. This country is a big tech player in the market.

Moreover, the insights of this work may also be applied to develop other sets of DPbD guidelines for different case studies and emerging trends in the e-health sector, such as telemedicine and telecare or e-referrals and m-apps. Every e-health technology has its own specific processing characteristics, but the GDPR remains the applicable legal framework and the main source of rules at the EU level.

Future research may include the use of AI and Big Data in the e-health context. AI algorithms are used for clinical care and medical research, for predictions and targeted healthcare provision. The aim is to provide personalised treatment and potentially prevent diseases. However, privacy and data protection concerns of this automated processing, including how to apply DPbD and protect data subjects' rights, should be addressed with an interdisciplinary approach by legal and technical scholars.

Finally, it might be worth investigating how to apply DPbD obligation to ensure secondary uses of data concerning health in medical research projects. These types of processing should still protect the rights and freedoms of data subjects when data are pseudonymised. At the same time the research could benefit public health and innovation. The secondary use of health data for research purposes is becoming increasingly important: the rights of the individual need to be balanced with the public interest in public health, following the necessity and proportionality principles.

This book attempted to show that the interaction between law and design could address some problems in the existing EU legal framework and in the particular e-health context. Data protection by design is and remains an intriguing legal concept that requires a technical implementation. This research is a piece of the puzzle, but there is still a lot of work to be done.