Alma Mater Studiorum - Università di Bologna
in cotutela con University of Luxembourg - Universitè du Luxembourg

DOTTORATO DI RICERCA IN

LAW, SCIENCE AND TECHNOLOGY

Ciclo 35

Settore Concorsuale: 12/H3 - FILOSOFIA DEL DIRITTO

Settore Scientifico Disciplinare: IUS/20 - FILOSOFIA DEL DIRITTO

BIG DATA IN HEALTH IOE IN EMERGENCY SITUATIONS: BETWEEN THE RIGHT TO PRIVACY AND DIGITAL HEALTH INNOVATION

Presentata da: Aiste Gerybaite

Coordinatore Dottorato

Monica Palmirani

Supervisore

Ugo Pagallo

Supervisore

MARTIN THEOBALD

Co-supervisore

Monica Palmirani

Esame finale anno 2023

PhD-FSTM-2023-023
The Faculty of Science, Technology and Medicine

DISSERTATION

Presented on 30/03/2022 in Bologna, Italy

to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG

EN INFORMATIQUE

by

Aiste GERYBAITE
Born on 18th June 1990 in Lithuania

BIG DATA IN HEALTH IOE IN EMERGENCY SITUATIONS: BETWEEN THE RIGHT TO PRIVACY AND DIGITAL HEALTH INNOVATION

Abstract

The unprecedented use of digital technologies in healthcare in the past five years in Europe has led to increased concerns regarding individual privacy and data protection. The increased use of digital health technologies in the past three years on the European continent due to the Covid-19 pandemic has exasperated these concerns, especially considering the processing and management of personal and sensitive data by public authorities in various Member States. These concerns raised a question on how individual and group privacy and related data protection rights can be adequately ensured in sensitive healthcare situations, such as a public healthcare crisis.

The chapters of the thesis pursue an answer to this question, focusing on a limited variety of selected themes in EU privacy and data protection law. Chapter 1 sets out the general introduction on the research topic. Chapter 2 touches upon the methodology used in the research. Chapter 3 conceptualises the basic notions from a legal standpoint. Chapter 4 examines the current regulatory regime applicable to digital health technologies, healthcare emergencies, privacy, and data protection. Chapter 5 provides case studies on the application deployed in the Covid-19 scenario, from the perspective of privacy and data protection. Chapter 6 addresses the post-Covid European regulatory initiatives on the subject matter, and its potential effects on privacy and data protection. Chapter 7 is the outcome of a six-month internship with a company in Italy and focuses on the protection of the fundamental rights through common standardisation and certification, demonstrating that such standards can serve as supporting tools to guarantee the right to privacy and data protection in digital health technologies.

The thesis concludes with the observation that finding and transposing the European privacy and data protection standards into scenarios, such as public healthcare emergencies where digital health technologies are deployed, requires rapid co-ordination between the European Data Protection Authorities and the Member States to guarantee that individual privacy and data protection rights are ensured. It observed that with the introduction of AI-based digital health technologies, the protection of the fundamental rights to privacy and data protection will remain a topical subject, with the need to work on harmonising different applicable regulatory regimes to ensure regulatory clarity.

Acknowledgements

First, I would like to express my sincere gratitude to the board of Law, Science, and Technology (Last-JD) PhD programme for the opportunity to form part of this extraordinary PhD experience.

I would like to thank my supervisor prof. Ugo Pagallo from the University of Turin for the continuous support, reviews, thoughtful comments, and recommendations on this dissertation. I would also like to express my gratitude to prof. Martin Theobald for continuous support in this PhD journey and especially while being a visiting PhD fellow at the University of Luxembourg.

My sincere gratitude goes to prof. Monica Palmirani, the supervisor of the PhD programme and the person without whom this PhD programme would not succeed in the first place.

I would like to thank my PhD colleagues who supported and went through this experience with me.

Finally, my heartfelt thank you goes to Roberto, who has continuously supported me during the past three years and stood by my side.

TABLE OF CONTENTS

ABSTRACT **1**

ACKNOWLEDGEMENTS **2**

1 GENERAL INTRODUCTION **5**

1.1 Living "Smart": Digital Health Technologies 5
1.2 Thesis Problem Statement 12
1.3 Thesis Objectives 14
1.4 Thesis Outcomes 15
1.5 Scope and Outline of the Thesis 15
1.6 Impact and Innovation 16
1.7 Publications and Research Activity 17

2 METHODOLOGY **18**

2.1 Research Structure and Notes on Methodology 18
2.2 Thesis Outlook 21

3 UNDERSTANDING BIG DATA, HEALTH TECHNOLOGIES, AND HEALTHCARE EMERGENCIES **25**

3.1 Introduction to Big data and its Attributes 25
3.2 Beyond the 3Vs of Big Data: Value as a Fundamental Attribute 27
3.2.1 On the Notion of Big data in the European Healthcare Context 28
3.2.1.1 Observations on Big data in the European Privacy and Data Protection Context 30
3.2.2 On Big Data-Driven Healthcare: The Advantages and Risks of Big Data 32
3.3 On the Notion of Digital Health Technologies 35
3.3.1 A Taxonomy of Digital Health Technologies for Health Emergencies 39
3.4 On the Notion of Healthcare Emergency: A Multi-Dimensional Nature of Emergency 45
3.5 Conclusive Remarks 50

4 REGULATIONS SURROUNDING DATA PROTECTION, BIG DATA, AND DIGITAL HEALTH TECHNOLOGIES **52**

4.1 Introduction to the Regulatory Landscape 52
4.2 Right to Privacy and the Right to Data Protection in the Context of Human Rights 54
4.2.1 On the Protection of the Right to Privacy and the Right to Health at the International Level 54
4.2.2 On the European Approach to the Right to Health, the Right to Privacy, and the Right to Data Protection 55
4.2.3 On the Evolution of the Right to Privacy and the Right to Health 56
4.3 Critical Analysis of Selected Data Protection Related Issues in the Context of Big Data and Digital Health Technologies 56
4.3.1 The Importance of Personal Data in Big Data and Digital Health Technology Context 57
4.3.2 The importance of Data Concerning Health and Article 9 in Big Data and Digital Health Technology Context 60
4.3.3 The Significance of the Data Protection Impact Assessment for Digital Health Technologies and Big Data 64
4.4 Ensuring Data Protection in Digital Health Technologies Through the Medical Devices Regulations Regulatory Framework 68
4.4.1 MDR at the Core of Digital Health Technology Regulatory Regime in the EU 68
4.4.2 The Evolving Nature of Medical Devices 69
4.4.3 Qualification as a Medical Device Versus Classification of a Medical Device 71
4.4.4 The Blurred Line Between Digital Health Technologies and Medical Devices: The Case of Intended Purpose 72
4.4.5 Establishing Mechanisms of Legal Coordination and Co-requisite Approach for Digital Health Technologies 74
4.5 Conclusive Remarks 78

5 REGULATING PUBLIC HEALTHCARE EMERGENCIES: BALANCING THE EU CITIZEN'S RIGHTS TO PRIVACY, DATA PROTECTION, AND THE RIGHT TO PUBLIC HEALTH **81**

5.1 The Current State of Play: Using Digital Technologies in Healthcare Emergencies. Balancing Fundamental Rights with Limited Competences and National Diversions 81

5.2 A Taxonomy of the Covid-19 Applications 83
5.3 Crisis Management with Digital Technologies: First-generation Covid-19 applications 85
5.3.1 Information Applications 85
5.3.2 The Case of Contact-Tracing Technologies 85
5.3.2.1 Contact-Tracing Technologies: Balancing the Right to Data Protection and Public Safety During the Covid-19 Pandemic 87
5.3.3 Surveillance Applications of Individuals in Quarantine 92
5.4 Crisis Management with Digital Technologies: Second Generation Technologies 96
5.4.1 The Deployment of Proofs of Vaccinations in the EU 96
5.4.2 A Case Study of the Estonian "Immunity Passport" Application 100
5.4.3 Other mHealth Technologies 102
5.5 Incentivising the Use of Data in the Covid-19 Pandemic Scenario 102
5.6 Responding to Crisis via Crisis Preparedness: EU's Proposal for the Regulation on Serious Cross-Border Threats to Health 103
5.7 Conclusive Remarks 107

6 EUROPEAN REGULATORY INITIATIVES: A WAY FORWARD TO ENSURE THE RIGHT TO PRIVACY AND DATA PROTECTION IN AI-POWERED DIGITAL HEALTH TECHNOLOGIES? 109

6.1 An Excursus on the European Health Union and on the EU Digital Decade 2030 111
6.2 The European Data Strategy: on the Proposal for the Creation of the European Health Data Space 114
6.3 From Big data Powered Digital Health Technologies to AI-Powered Digital Health Technologies: Implications of the Proposal for the Regulation of Artificial Intelligence 121
6.3.1 Background on the AI Act Proposal 121
6.3.2 The Criticism and the Appraisal 124
6.3.3 Digital Health Technologies as High-Risk AI Systems in the AI Act Proposal 126
6.3.3.1 Integrating Regulated and Unregulated Digital Health Technologies with AI Regulation 128
6.3.3.2 The AI Act Proposal and Digital Health Technologies in Public Health Emergencies: A Missed Opportunity? 131
6.4 A Competitive Market: U.S. Approach to AI-based Digital Health Technologies 134
6.5 Do the European Regulatory Initiatives Ensure the Rights to Privacy and Data Protection in AI-Powered Digital Health Technologies? 136
6.6 Conclusive Remarks 138

7 GUARANTEEING THE RIGHT TO HEALTH AND THE RIGHT TO PRIVACY IN DIGITAL HEALTH TECHNOLOGIES: CYBERSECURITY, COMMON STANDARDS, AND CERTIFICATIONS 140

7.1 Privacy Preservation in Digital Health Technologies: Focus on the EU Cybersecurity Act, Standardisation, and Certifications 142
7.2 Common Cybersecurity Certifications for Digital Health Technologies 144
7.3 Certification and Standardisation Under the AI Act Proposal: Impacting Digital Health Technologies? 148
7.4 Cybersecurity Standards, Guidelines, and Third-Party Certifications for Digital Health Technologies: Multi-layered Relationship 149
7.4.1 ISO Cybersecurity Certifications for Ensuring Privacy in Digital Health Technologies 152
7.4.1.1 Data Protection Specific Standards and Certifications 156
7.4.2 Standardisation and Certification of Digital Health Technologies in Public Health Emergencies 160
7.5 Between Europe and the U.S.: Diverging Approaches to Standardisation and Certification of Digital Health Technologies 162
7.6 Conclusive Remarks 166

8 CONCLUSIONS 168

8.1 Review of Background and Problem Questions 168
8.2 Review of Analyses and Findings 172
8.3 Final Observations and Possible Future Research Directions 180

9 BIBLIOGRAPHY 181

10 ANNEXES 200

1 General Introduction

1.1 Living "Smart": Digital Health Technologies

The setting of this thesis intertwines the augmented utilisation of big data and artificial intelligence- (henceforth, "AI") based digital health technologies in modern society. Big data, AI, and the Internet of Everything (henceforth, "IoE") have been vastly applied in many domains. For example, in the sports domain big data is used to track scoring and predicting game outcomes, whilst in healthcare big data is used to track patients' health status, predict disease outbreaks, or manage health emergencies at both individual and public levels. Sophisticated IoE devices are now able to process big data to monitor undesirable events through real-time alerting, such as the crash of vital signs with wearable wireless sensors, domestic accidents involving elderly people, or distribution of ambulances and availability of hospitals. Also, sophisticated machine learning and AI-based digital health technologies have only recently gained traction. Such technologies have started to pave the way towards a more predictable healthcare by, for example, assisting healthcare professionals in X-Ray or ECG test interpretations. Even our daily lives are submerged in various digital health-related applications and devices, allowing us to track our sleep, diet, menstrual cycles, and improve overall health.

While the progress of big data and artificial intelligence dates back to the twentieth century, the last fifteen years have seen the rise of powerful new digital health technologies integrating big data and AI. Machine learning based on statistical correlations found in big data can now make probabilistic determinations about one's health. With the advent of quantum computing, quantum-enhanced machine learning techniques hold the promise of more accurate and more granular health risk predictions. Precision medicine, based on personalised interventions and treatments with optimal prices for the patient is considered the future of digital healthcare.

Digital health technologies are a broad, multi-disciplinary notion and a concept that lies at the intersections between technology, law, and healthcare. Digital health technologies, as the notion suggests, are applied in the healthcare industry, and can incorporate hardware, software, and health services. Digital health technologies are an umbrella term that include mobile health (henceforth, "mHealth") applications, medical devices, electronic health records (henceforth, "EHR"), wearables, telehealth, and digitally personalised healthcare assistance. The notion is also related to terms such as health IT, healthcare analytics, medical technology, or healthcare informatics.

Digital health technologies in the field of healthcare emergencies can range from regulated medical devices that can predict vital sign issues such as implantable heart medical devices, blood

sugar measuring devices, to an abundance of mHealth applications capable, for example, of tracking every imaginable health aspect and generate millions of individual data points, specifically, personal sensitive data points regarding health of an individual.

Digital health technologies for healthcare emergencies do not only cover personal health emergencies. Such technologies are also deployed in public health emergencies. Recent global events, namely, the Covid-19 pandemic, have shown that big data and AI-powered digital health technologies may also be applied in healthcare emergencies. The application of such technologies may carry an enhanced risk to the health society at large, or an immediate risk to health of an individual and therefore require urgent intervention to prevent a worsening of the situation or to mitigate possible lethal consequences. The OECD has observed that digital health transformation is a political choice, and that the Covid-19 pandemic has created an opening for a meaningful reform, to move away from uncoordinated and siloed approaches to health data to realise strategic governance of health information systems.

The Covid-19 crisis did indeed provide an opening for the Union to address issues within digital healthcare technologies' sector to take advantage of fully utilising such technologies and their data. It served as a "cataclysmic" event that improved governments' responses to the accessibility of personal health data, health data management, regulatory and policy frameworks applicable in the digital health technology industry (see Table 1, below)[1].

[1] Francesca Colombo, Jillian Oderkirk and Luke Slawomirski, 'Health Information Systems, Electronic MedicalRecords, and Big data in Global Healthcare: Progress and Challenges in OECD Countries' [2020] Handbook of Global Health 1.

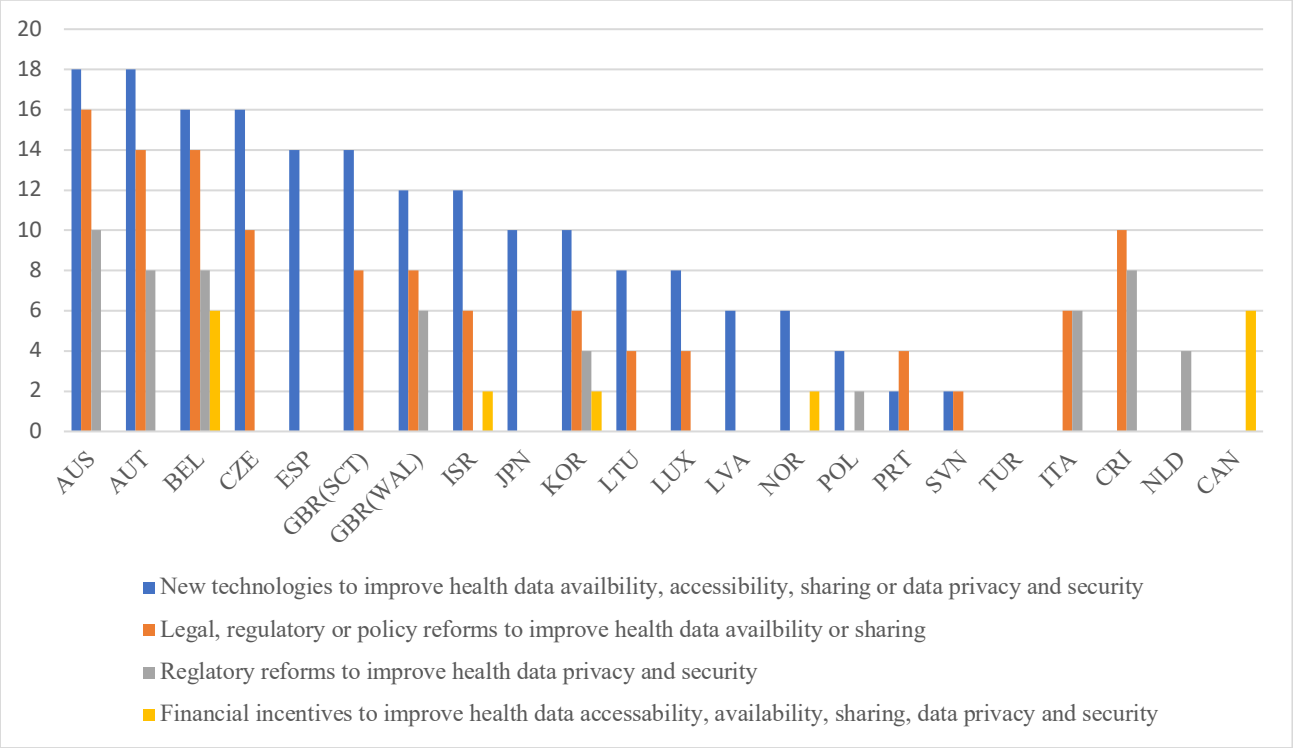

Table 1. Changes to health data governance because of Covid-19 pandemic. Source: OECD, Questionnaire on Health data and governance changes during the COVID-19 pandemic, 2021.

Considering the broad range of digital technologies used in healthcare, stakeholders also include a broad range of persons, and entities. Specifically, stakeholders in digital health technologies include governments, patients and users, whose well-being may depend on such technologies, doctors, and other healthcare practitioners prescribing such technologies, researchers, developers, and manufacturers of digital health technologies[2]. Patients and other users of such digital health technologies, such as doctors or hospital personnel, often lack access to personal health data, affecting rights of such individuals. As observed by the OECD research, seeking information online, including accessing personal health information "more than doubled between 2008 and 2017"[3] (see Table 2, below).

[2] Proposal for a Regulation of the European Parliament and the Council on the European Health Data Space COM(2022) 197 final 2022 (European Commission) 1.

[3] 'Digital Health - OECD' <https://www.oecd.org/health/digital-health.htm> accessed 28 July 2022.

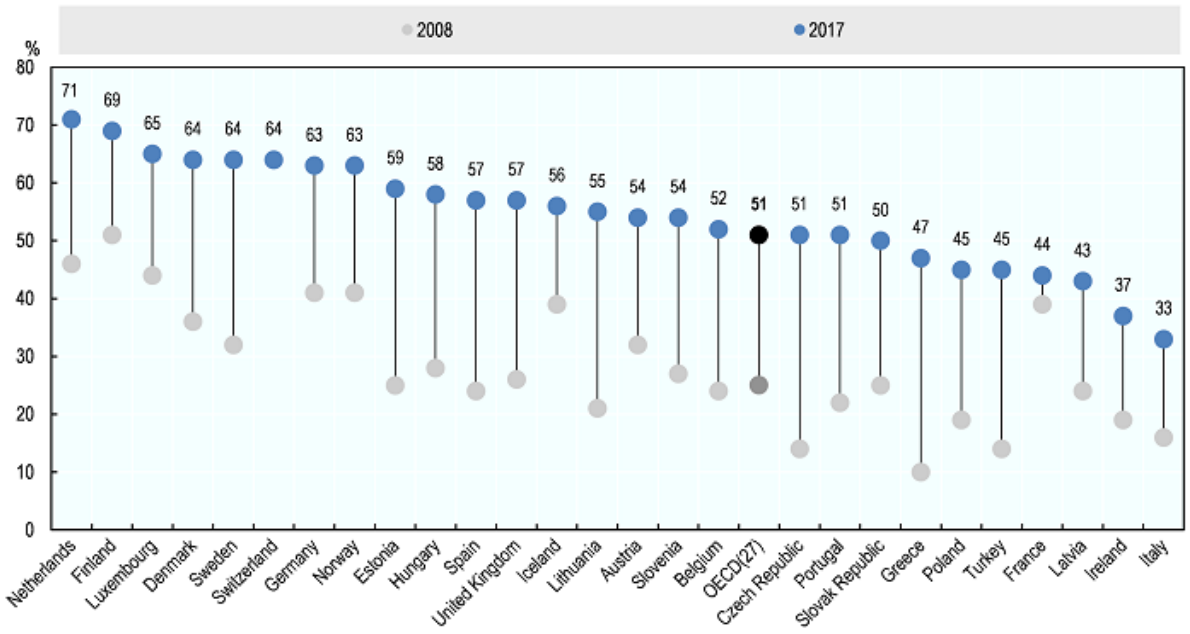

Table 2. Access to health information online between 2008 and 2017. Source: OECD[4].

These individual rights are further affected by personal data breaches such as unauthorised disclosure of special categories of data, for example, as in the recent Dedalus Biologie data leak[5], or misuse of special categories of data for purposes other than the one(s) agreed by data subjects.

The success of digital health technologies can be primarily associated with big data and machine learning methods, and their increased availability, and interoperability. Data is now available from various sources such as social media, and sensor monitoring technologies. For example, street cameras and digital devices or governments, such as in the case of hospital-stored patient healthcare records. These records are often combined in data pools, which may be interconnected with other data pools, processing and sharing data, occasionally without consent of the person involved, known as the data subject, in accordance with the EU General Data Protection Regulation (henceforth, the "GDPR").

Furthermore, whilst some of the healthcare emergencies are self-evident and more predictable, other incidents, such as public healthcare crises (e.g., disease outbreak), require statistical data and long-term observations to decide whether a situation qualifies as a healthcare emergency from both an empirical and legal standpoint.

While the opportunities of big data and AI-powered digital health technologies can provide ample good to society, such predominantly data driven technologies lead us into uncharted waters, bringing about unexpected risks.

[4] Colombo, Oderkirk and Slawomirski (n 1).

[5] 'Health Data Breach: DEDALUS BIOLOGIE Fined 1.5 Million Euros, CNIL' <https://www.cnil.fr/en/health-data-breach-dedalus-biologie-fined-15-million-euros> accessed 17 May 2022.

The convergence between various digital health technologies, smart devices, data, and AI poses risks to both individual and society. On the one hand, public organisations may be tempted to exploit their ever-reaching powers and use AI and big data to pursue legitimate objectives to improve public healthcare or survey individuals via pervasive monitoring and limiting their freedoms, leading to life in the so-called "surveillance state".

On the other hand, private organisations may exploit big data and AI to achieve legitimate economic objectives. Nonetheless, they may also abuse their power over personal data when achieving such objectives. Furthermore, the public-private sector initiatives may cause the largest risks as such initiatives may have the power to harvest the vast data pools, merging them, obtaining even more insight, leading to widespread interference to personal privacy or even to breaches of personal data protection rights.

In time-sensitive situations, such as healthcare emergencies, the use of big data and AI-based digital health technologies also poses several questions, with respect to the precise definition of a healthcare emergency, the agencies involved, and the procedures used, which may require the use of sophisticated instruments such as IoE solutions to detect whether a situation qualifies as an emergency both from empirical and legal perspectives. This is of particular significance as the legal qualification of a healthcare emergency may also vary depending on jurisdictions. In public healthcare emergencies, large amounts of data may be required to predict the spread of diseases or to manage such emergencies, as we have seen in the case of the Covid-19 pandemic.

In addition, big data obtained from multiple sources, such as smart watches or healthcare records, requires careful analysis from the perspective of privacy and data protection[6]. For example, research has already extensively addressed whether big data used in healthcare can be considered as personal under the applicable EU regulatory regime, and, if so, to what extent. In fact, there is a common understanding by the data protection community as regards to big data that, in situations where big data is not anonymised, such data falls under data protection law. Arguably, even pseudonymised big data falls under data protection laws; however, this is still debatable as it depends on the anonymisation techniques applied, considering advances such as quantum computing in data pseudonymisation.

Furthermore, current research in healthcare tends to pay more focus on the development of the technological solutions for the sector, on, for example, various medical devices, or the regulatory requirements applicable to the sector. Nevertheless, the impact of big data and AI algorithmic advancements on the fundamental rights to personal data protection and their effect vis-à-vis the right to health tends to be a constant debate in the research. In fact, sometimes, data protection

[6] Amandine Scherrer Gloria González Fuster, 'Big data and Smart Devices and Their Impact on Privacy' [2015] European Parliament, Study of the LIBE Committee.

research explores data protection-related issues in a sort of legal 'vacuum', measuring it as an absolute right and rarely paying attention to how these rights can affect the fundamental right to health.

In public healthcare emergencies, legal risks range from the legal grounds for processing big data in terms of the GDPR, to ensuring privacy and personal data protection in processing of big data itself, particularly in sensitive scenarios such as healthcare emergencies.

In exceptional healthcare situations, such as the Covid-19 pandemic, the relationship between healthcare emergency, fundamental rights to privacy, data protection, and the right to health become even more complicated. The Covid-19 pandemic presented an unprecedented event, a healthcare emergency both at EU and international levels that required an intervention and collaboration of all the Member States of the EU. Therefore, balancing these rights in a complex situation, such as of Covid-19, required careful assessment and evaluation of these rights[7,8]. The evaluation of these rights should be examined considering the GDPR for both public health purposes and in cases of health emergencies, since the health-related data legal basis stems from Article 9 of the GDPR. Specifically, Article 9(2)(c) allows processing data where the "processing 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"[9].

Furthermore, GDPR Article 9(2)(g) provides for the processing of data related to health for reasons of "substantial public interest", based in EU or the Member State law. In all cases, any processing of data must be proportional "to the aim pursued"[10] and respect the provisions of the GDPR. Article 9(2)(i) also permits the processing of personal health data in cases of "public interest in the area of public health"[11]. Finally, Article 9(2)(h) permits the processing of personal health data for, amongst others, "scientific research purposes"[12], which are essential in cases of healthcare emergencies such as the Covid-19 pandemic, in accordance with Article 89(1) based on EU or national law, where proportionality of the processing and respect of the rights enshrined in the GDPR is ensured.

Apart from the GDPR, the interaction of other laws for the deployment of digital health technologies in public healthcare emergencies also play a role in ensuring privacy and data protection when such digital health technologies are deployed. For example, the proposed

[7] 'Covid-19: A New Struggle over Privacy, Data Protection and Human Rights? – European Law Blog' <https://europeanlawblog.eu/2020/05/04/covid-19-a-new-struggle-over-privacy-data-protection-and-human-rights/> accessed 7 July 2020.

[8] Ugo Pagallo, 'Sovereigns, Viruses, and the Law: The Normative Challenges of Pandemic in Today's Information Societies' [2020] SSRN Electronic Journal.

[9] The European Parliament and The Council, Regulation (EU) 2016/679 of the European Parliament and 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 2016.

[10] ibid.

[11] ibid.

[12] ibid.

regulation on Serious Cross-Border Threats to Health[13], EU industry specific legislation such as the Medical Devices Regulation[14] (henceforth, the "MDR"), cybersecurity legislation such as the NIS2 Directive, and the Cybersecurity Act ought to be considering, as well as the proposal for the Artificial Intelligence Act[15] (henceforth, "AI Act proposal"), and the proposal for the creation of the European Health Data Space[16], the fact that all may affect the deployment of digital health technologies in healthcare emergencies.

Finally, in public health emergencies, the deployment of digital health technologies may also be subject to specific national provisions, such as in the case of the deployment of technologies for the Covid-19 pandemic management, as will be observed further in Chapter 5. Navigating the spider's web of EU and national rules applicable in healthcare emergencies proves a challenge, as it requires the European Union and the Member States to carefully consider which digital technologies to deploy, when to deploy them, and how to ensure citizen protection against breaches to fundamental rights, such as the right to privacy, data protection, and the right to health.

To complicate this research topic even further, current research tends to overlook the two dimensions of healthcare emergencies: individual health emergencies and public health emergencies. Researchers often focus mainly on digital health technologies deployed for individuals and individual health emergencies. For example, technologies used to track loss of vital signs by an individual which would not qualify as a public health emergency but, nonetheless, could have a devastating impact on an individual's wellbeing.

The deployment of digital technologies in public health emergencies is often a less researched area. The public dimension of healthcare emergencies refers to emergencies such as global outbreaks of diseases, for example, the Covid-19 virus as well as severe acute respiratory syndrome (henceforth, "SARS"). These two distinct scenarios may carry with them different personal data protection implications. Accordingly, there is a constant struggle of the law lagging behind technology and the implementation of the law in technology scenarios is not straightforward. As the ethical-legal research world focuses on fostering a high-level discussion on big data, AI, healthcare, and IoE, the ICT sector wonders what all this means to their specific scenario.

---

[13] European Commission, Proposal for a Regulation of the European Parliament and the Council on serious cross-border threats to health and repealing Decision No 1082/2013/EU 2020.

[14] OJ L 117, Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance.) 2017 176.

[15] The European Parliament, Proposal for a Regulation of the European Parliament and of the Council laying dow harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts COM/2021/206 final 2021.

[16] European Commission, Proposal for a Regulation on the European Health Data Space (Text with EEA relevance) 2022.

The research therefore investigates the complex relationship between big data, AI, privacy, and data protection in digital health technologies developed and deployed for public health emergencies. In this thesis, the research aimed at providing an in-depth analysis of the applicable regulatory regime for the use of such technologies in public healthcare emergencies and the translation of the regulatory regime into specific public healthcare scenarios, and the deployment of the Covid-19 crisis related digital health technologies in the EU. Lastly, the thesis provides observations as to how the deployment of digital health technologies in the Covid-19 pandemic affected the perception of the right to privacy, data protection, and the right to health in the digital environment.

1.2 Thesis Problem Statement

The European Union is undergoing a shift in its data strategy with the introduction of new initiatives such the new Common EU Data Space and the EU Commission's Digital Decade Strategy 2030. Despite these initiatives, the current European regulation of data, including big data in healthcare and AI, the regulatory landscape can be compared to a spider's web consisting of multiple layers and intricate correlations between multiple pieces of legislation[17].

The complexity of the digital health technologies and data protection regulatory landscapes makes it challenging to assess whether in healthcare emergencies a balance amongst the right to privacy, the right to personal data protection vis-à-vis the right to health can be and is maintained. Research tends to argue that in such situations the right to health takes the more prominent role, as a healthcare emergency poses a direct and imminent threat to life. Conversely, in situations such as public health emergencies, and the preparedness for such public health emergencies, such as the Covid-19 pandemic, the balance between the right to data protection and the right to health are trickier to assess and maintain. This is especially relevant in the scenario of health crisis preparedness where vast amounts of data are necessary to, first, predict, and second, prepare for the public health crises.

Furthermore, with the digitalisation of healthcare and the growth of mHealth and eHealth devices used for management of patient health and public healthcare emergencies, patients are encouraged to share vast amounts of their personal and personal sensitive data not only with health professional but also with unwanted third parties. While the use of mHealth and eHealth devices bring undoubted benefits to the healthcare sector and the patient, underlying privacy, and data protections risks, particularly in public healthcare scenarios, ought to be addressed.

With the above background in mind, the thesis problem statement is divided into four main

[17] For example, consider the Medical Devices Regulation and the proposal for AI Act's potential overlap as to assessment of both technologies and overlapping requirements for such assessments.

question groups that the thesis explores through its chapters:

1. How is big data conceptualised and what is its relationship with digital health technologies and public healthcare emergencies?

In this respect, Chapter 3 of the thesis, being the first chapter of the body of the thesis, explores and analyses the notions of big data, digital health technologies, and healthcare emergencies. The analysis and search for the first answer allows the research to depict an accurate portrait of the regulatory complexity of addressing legislation and policy initiatives in the digital health technologies sector that is often 'lost in translation' due to lack of common understanding of the above-mentioned notions.

2. To what extent are the current and the proposed EU regulatory initiatives able to ensure the right to privacy, and specifically the right to data protection considering digital health technologies?

   a. To the extent where the current EU and the proposed regulatory initiatives fall short in ensuring privacy and data protection, are there other ways to improve the legislative proposals and the current regulatory framework?

Considering the second question and its sub-questions, Chapters 4 and 6 in conjunction search for an answer to this question. The answer to the question is sought through a comprehensive study of the applicable regulatory privacy, personal data protection, digital health technologies, and AI frameworks in the EU and the suggested regulatory proposals for the latter at the EU level.

Chapter 6 first delves into the future regulatory landscape for digital health technologies, specifically addressing the proposal for AI regulation and the regulation for the creation of the European Health Data Space. This chapter draws knowledge from the AI Act proposal requirements that would be applicable to AI-based digital health technologies with the requirements already enshrined in the MDR, drawing parallels, establishing overlaps, and potential contention points between the two regulatory frameworks. Also, a comparative view is also drawn from the perspective of the U.S. applicable regulatory framework, being the top competing jurisdiction for digital health technologies.

3. Considering the specific nature of public health emergencies, such as the Covid-19 pandemic, and the rights to health, the right to privacy, and specifically data protection, in sensitive situations such as public healthcare emergencies, how are such rights balanced?

Considering the third question and its sub-questions, Chapter 5 of the thesis provides a response. This chapter in particular analyses a number of case studies of the Covid-19 applications deployed during the pandemic both at European and national levels. It provides an in-depth analysis of how the balance between the right to health and the right to privacy was maintained in the deployment of such technologies. The chapter finishes with final observations on the new proposal for regulation on Cross-Border Threats to Health at the European level and its impact to the above-mentioned rights considering preparedness for future public health threats.

4. Ultimately, considering the risk to privacy and data protection in digital health, how can common standardisation and certification of digital health technologies ensure compliance with the applicable privacy and data protection legislation to minimise such risks?

Chapter 7 addresses this final question. Chapter 7 delves further into an in-depth analysis of the common standards and certification set at the European level as enshrined in the currently applicable legislation such as the Cybersecurity Act and the NIS2 Directive. The chapter then narrows down its scope to the internationally accepted standards and certifications, focusing on the International Organisation for Standardization (henceforth, "ISO") and the International Electrotechnical Commission (henceforth, "IEC") ISO 27000 standard family standards that address privacy, and by extension partially data protection, and GDPR specific standards such as ISDP10003. This Chapter analyses specifically the application of the above-mentioned standards in a particular case study, the development of a data sharing platform. The platform encompasses hospital-held personal health data, mHealth and telehealth-transmitted personal health data for primary purposes of patient treatment and monitoring, and the potential use of such data for secondary use, including research for health crisis preparedness. Said Chapter 7 is the outcome of the 6-month internship at a company in Turin, Italy, which is developing the above-mentioned platform.

Lastly, the findings of this thesis are aimed at benefiting different stakeholders to facilitate the building of a digital technologies market that is competitive and based on the European values.

1.3 Thesis Objectives

With the thesis background and problem statement in mind, the thesis addresses some of the selected legal issues related to privacy and personal data in Europe. It considers these issues in the context of public healthcare emergencies and digital health technologies, while examining the current and the proposed regulatory and policy initiatives. The articles that the thesis author cites in parts of her consideration herein consider the complex relationship between the fundamental

right to privacy, data protection, and the right to health in public health emergencies.

The analysis aims to showcase that the balancing of the fundamental rights to health, privacy and data protection ought to be maintained in the digital world, when deploying digital health technologies in public healthcare emergencies. It aims to establish that the balancing of these rights should take the fundamental role in public healthcare emergencies. This is because public healthcare emergency scenarios may become the perfect contextual situations for proclaiming public health emergencies which would allow certain fundamental rights of individuals (such as the right to data protection) to be lawfully denied.

Furthermore, the research also demonstrates that Europe lacks jurisdictions such as the U.S. has in the deployment of AI in digital health technologies and harvesting AI potential, and also its "knowledge" in situations such as public health emergencies and preparedness for such public health emergencies.

The contribution to the knowledge in the research domain is achieved through an investigative legal analysis of the applicable privacy and data protection frameworks to the extent they are applicable to digital health technologies within the European Union.

1.4 Thesis Outcomes

In this respect the thesis provides several outcomes:

1. Conceptual analysis of the notions of big data, emergency in healthcare, and digital healthcare technologies from a legal point of view.
2. A comprehensive overview of the regulatory framework surrounding big data and AI-powered digital health technologies in the European Union from privacy and data protection perspectives. In this respect, the thesis establishes the extent to which the current regulatory regime within the EU applies to big data-powered digital health technologies, the shortcomings of the current regulatory regime, and the future of the regulation of digital health technologies.
3. Analysis of the selected digital health technologies used in healthcare emergencies from the perspective of balancing the right to health with the right to privacy and data protection.

1.5 Scope and Outline of the Thesis

The scope of this thesis is limited to legal and technical considerations related to the use of big data and AI-powered digital health technologies from the perspective of the right to health, the right to

privacy and data protection. In terms of its scope, the thesis discusses European laws relevant to privacy, personal data, digital health technologies, and healthcare emergencies. In this respect, the analysis is centred on the General Data Protection Regulation and its relationship with the Medical Device Regulation, Cybersecurity Act, the Network and Information Security Directive, the proposals for the regulation of Artificial Intelligence Act, the proposal for the European Health Data Spaces regulation, and the EU proposal for the regulation of the Cross-Border Threats to Health.
Specifically, the thesis chapters:

i. Attempt a critique on the notion of big data, health emergencies, and digital health technologies in EU laws;

ii. Examine the state of the art of the legal regulatory regime surrounding digital health technologies, big data, and healthcare emergencies in the EU;

iii. Discuss how the potential policy and regulatory attempts at the EU level may be the tools to reconcile the benefits of big data and AI-powered digital health technologies with the rights to privacy and data protection and attempt to provide suggestions on the improvement to the proposed policies and regulations;

iv. Analyse digital health technologies deployed in the context of the Covid-19 health emergency in relation to the rights to privacy, data protection, and the right to health;

v. Demonstrate how technical solutions, specifically privacy-preserving and enhancing technologies, may be used as instruments and solutions that aim to ensure and guarantee the fundamental rights to privacy and data protection without hindering the right to health.

1.6 Impact and Innovation

The legal debate tends to overlook the increasing number of various digital health technologies used within the healthcare sector. It tends to underestimate the power of big data and AI in healthcare and the influence it may have on the citizen's fundamental rights to privacy, data protection, and to health.
Similarly, the technology sector fails to grasp the necessity to apply underlying fundamental principles to their solutions, and the practical application of the regulatory regime.
Therefore, the inter-disciplinary approach of the thesis works on addressing the above to bridge the gap between the legal and the technology sectors and to benefit the wide range of stakeholders including legislators, scholars, and practitioners.

1.7 Publications and Research Activity

This thesis is based on three years of in-depth research and a collection of publications focused on the balancing of personal data in healthcare emergencies, and the use of digital health technologies for the governance of public healthcare emergencies, namely the Covid-19 pandemic. The thesis is largely based on peer-reviewed publications:

i. Aiste Gerybaite, Francesco Vigna, Sofia Palmieri, December 2022: "Equality in Healthcare AI: Did Anyone Mention Data Quality?". Rivista di BioDiritto – BioLaw Journal (ISSN 2284-4503).

ii. Aiste Gerybaite, October 2021. "Digital Governance: The Case of Proofs of Vaccinations". In proceedings of the 14th International Conference on Theory and Practice of Electronic Governance (pp. 450-454), published by ACM.

iii. Aiste Gerybaite, December 2021."Big data in IoE in healthcare emergencies: analysis of autonomous emergency response systems in healthcare emergencies". Publication at the Doctoral Consortium of the European Association for Health Law, European Association for Health Law official newsletter (ISSN 2708-2784).

iv. Aiste Gerybaite and Paola Aurucci, June 2020. "Big data and Pandemics: How to strike the balance in times of GDPR?" Intelligent Environments 2020: Workshop Proceedings of the 16th International Conference on Intelligent Environments.

v. Aiste Gerybaite, February 2021."Country report: health system in Lithuania", European Association for Health Law official newsletter, (ISSN 2708-2784).

vi. Aiste Gerybaite, December 2020. "Big data in IoE: investigating IT approaches to big data in healthcare whilst ensuring the competing interests of the right to health and the right to privacy." The Proceedings of the 1st Doctoral Consortium at the European Conference on Artificial Intelligence (DC-ECAI 2020).

2 Methodology

A complex research topic often requires a complex methodology. While the field of legal philosophy provides methodological foundations for this thesis, the methodology also includes distinct methodological techniques in different chapters of the work. This chapter thus discusses the overall structure and methods of this dissertation. Following this, the next section discusses methods of investigation adopted in the single chapters.

2.1 Research Structure and Notes on Methodology

To answer the central questions of the thesis, the research employs interdisciplinary legal research methods to investigate, analyse and clarify privacy, data protection, and the right to health concerns posed by use of digital health technologies in healthcare emergency situations. While in-depth methodology is described at the beginning of each chapter of the thesis, this section provides an oversight of the methodologies used in the work.

Grounded on the work of legal scholars engaged in the philosophical inquiry on privacy and data protection, it allowed for insightful contributions to interpretation of systems of laws and their complex relationship with each other. Regardless of the ontological status of laws, the relevant perspectives from the field of legal philosophy focus on the epistemological, i.e., levels of observations or interpretation of a system (levels of abstraction)[18] and the notions of co-regulation and self-regulation[19].

Against this mise-en-scène, the thesis sets out the type of interdisciplinary research developed in this thesis. In general, the research is of a qualitative nature and is positioned at the intersections of:

a. EU fundamental rights law;
b. EU privacy and data protection law;
c. EU healthcare technology law;
d. Health informatics;
e. Cybersecurity law; and
f. Data ethics.

[18] Luciano Floridi, 'The Method of Levels of Abstraction' (2008) 18 Minds and Machines 303.
[19] Ugo Pagallo, Pompeu Casanovas and Robert Madelin, 'The Middle-out Approach: Assessing Models of Legal Governance in Data Protection, Artificial Intelligence, and the Web of Data' (2019) 7 Theory and Practice of Legislation 1.

Therefore, the use of purely legal research in the context of digital health technologies, while necessary, would not provide a comprehensive view of the issues in the field of research. The interdisciplinary research is thus necessary as it complements other research methods. The use of interdisciplinary research facilitates the creation of "knowledge on the development of a good functioning legal system, which does justice to the legal reality, on the one hand, and the actual reality on the other hand"[20]. The value of conducting an interdisciplinary research rest with the ability to better grasp the influences surrounding regulation can lead to a well-informed judgement of the legal norms and legal systems.

Knowledge generation is often pursued on the basis of study, observations, and comparison. Based on the objectives and nature of the subject matter of the research, this thesis makes use of both descriptive exploratory and comparative methods of research. Descriptive methodology refers to the methods that describe the characteristics of the variables in the research without focusing on the causal link of the phenomena or events. The descriptive method allowed the nature of societal events to be observed and reflected on, focusing on reflection questions. Considering explanatory research methods, the research used a "cause and effect" model that uncovered patterns and trends in the research for new insight.

With respect to the comparative method, this includes examining the mass of legal data, finding and assessing similar and different data points to arrive at revelations about the compared legal data[21]. However, simply comparing the letter of the law is not sufficient in the context of comparative legal research. Comparative legal research can cast partial light on the subject matter, as the law is intrinsically connected with social and cultural systems, that is, it is highly context-dependent, requiring the context to become the essence of any comparison[22].

In essence, all the chapters of the thesis include a blend of all the research methods. By systematically studying bodies of law through both doctrinal and non-doctrinal methods, it allowed the researcher to achieve the aims of this socio-legal study that aimed at understanding the impact of the legal systems on the social system.

The study reviewed articles, laws, policies, expert guidelines, opinions, and industry studies from several data sources. Despite the complexity of the topic, the research conducted a systematic literature review of the following trustworthy and acknowledged legal sources:

---

[20] Wendy Schrama, 'How to Carry out Interdisciplinary Legal Research. Some Experiences with an Interdisciplinary Research Method' (2011) 7 Utrecht Law Review 147.

[21] Edward J Eberle, 'The Methodology of Comparative Law' (2011) 16 Roger Williams University Law Review <https://heinonline.org/HOL/Page?handle=hein.journals/rwulr16&id=53&div=5&collection=journals> accessed 3 February 2022.

[22] Esin Orucu, 'Methodological Aspects of Comparative Law' (2006) 8 European Journal of Law Reform <https://heinonline.org/HOL/Page?handle=hein.journals/ejlr8&id=37&div=10&collection=journals> accessed 3 February 2022.

i. International and EU legal acts and accompanying legal interpretations adopted by the EU.

ii. National laws of selected EU Member States specific rules on the protection of personal data concerning the use of digital health technologies in healthcare emergencies.

iii. Healthcare specific policies and regulations, including expert guidance documents drafted at EU level.

For legal research, scientific literature from databases such as SSRN, Google Scholar, and Springer were reviewed. Non-academic literature included studies prepared by advisory companies as well as studies carried out by NGOs.

For the technical research, the materials were sourced from trustworthy and acknowledged databases such as ScienceDirect, Elsevier, IEEE Xplore, ACM Digital library, and SpringerLINK for scientific literature.

For both legal and technical research, a combination of keywords was identified:

1. for big data in healthcare: big data benefits and risks; big data applications in healthcare; digital health technologies; wireless wearable sensors; wearables.
2. for regulation of big data in healthcare: regulation of big data; privacy and data protection and big data; healthcare regulation and big data; GDPR and healthcare applications; medical devices; MDR.
3. for cybersecurity: cryptography; ISO standards; privacy by design; security by design; security of healthcare devices; blockchain for security.
4. for health technologies used: emergency response systems, health monitoring devices, surveillance tools, contact tracing, wireless sensors, biosensors, healthcare wearable devices.

From the sources resulting from the search, those most relevant to the research work were selected, based on four aspects:

1. Title;
2. Subtitle;
3. Abstract; and
4. Citation.

The research is aware of the wide range of the keywords chosen; however, such a selection was important to grasp the complexity and the interconnectivity of the law, science, and technology within the topic.

The research further selected the relevant materials which were based on the following criteria, i.e., articles with a particular focus on the legal aspects of data privacy, and data security in healthcare devices, and articles with a focus on the technical aspects on the design of such devices.
The research focused on reviewing the most up-to-date literature available. The literature review identified an existing gap in the research: the research tends to focus either on the development or improvement of the technological solutions for healthcare, for example, various medical devices, or on the regulatory requirements applicable to the sector. Yet, the impact of big data, privacy and data protection on the ICT applications tend to be overlooked.
Furthermore, to address the issue that the healthcare sector finds it hard to tackle the two dimensions of healthcare emergencies, the public healthcare and the individual healthcare emergency dimension, and its implications for data protection and privacy, a comparative analysis was carried out for the notions of emergency, big data, and health technologies in the context for the research, focusing on the international and EU provided definitions for both notions and the national interpretations of such notions.
To allow a comprehensive and interdisciplinary research, the thesis provides an analytical and descriptive mapping out of the regulatory framework surrounding big data and digital health technologies regulatory regime in the EU from the prism of privacy, data protection, and the right to health. The approach chosen focused on looking at big data in health legislation from a geographical perspective, focusing on the European Union. This allowed a systemic review of the legislation and an analysis of the legal and regulatory environments governing big data in healthcare, drawing conclusions on policy implications.
Through the mapping out of the regulatory regime, the researcher identified and delved into the existing legal issues in the field of big data with a focus on data protection. Such legal issues mainly focus on data protection under the GDPR such as processing of personal data in healthcare crisis or use of personal data processing technologies to manage health emergencies.
Through such mapping out the research was able to draw the context of the research in terms of the applicable regulatory regimes to big data tools in healthcare to refine the approach for other stages of the work.

2.2 Thesis Outlook

The thesis is divided into eight chapters. The first two short chapters cover the general introduction, research problem, research objectives, research outcomes, publications, presentations, workshops,

and related research activities, with Chapter 2 dealing with research structure, methodological remarks, and data sources.

Chapter 3 forms the first chapter of the body of the thesis. The chapter discusses and examines the basic concepts and notions of the research: big data, healthcare emergencies, and digital health technologies. The aim of this chapter is to critically reflect on the interpretations of such notions at the EU and international level. Drawing inspiration from the legislative definitions, the chapter suggests focusing on the features related to the notion of big data, namely the 3Vs. Critical observations are also drawn regarding the concept of healthcare emergency from both regulatory definitions available at the EU and national levels as well as the interrelation of the notion with the notion of the state of emergency as discussed by legal philosophers.

Chapter 4 analyses the regulatory framework applicable to big data, data protection, and digital health technologies. This chapter conceptualises the applicable regulatory regime starting with a historical observation and evolution of the rights to privacy, data protection, and the right to health. This historical background facilitates a further discussion of the regulatory framework regarding digital health technologies, big data, and data protection at the European level which includes both general and specific regulatory regimes. The chapter examines the interaction of privacy and data protection laws in digital healthcare technologies, and its impact on the big data and digital health technologies regulatory regime. As will be uncovered in Chapter 4, the influence of privacy and data protection law is apparent at all levels of regulation, making privacy and data protection the core fundamental rights. This chapter analyses several of the chosen issues related to big data in healthcare, notably the place of big data in the context of the GDPR's notions of personal data and data related to health. It also explores and stresses on the importance of a Data Protection Impact Assessment (hereafter, the "DPIA") in the processing of big data in healthcare, and the current piecemeal approach by the several Member States against the EDPB's guidance on big data processing.

Chapter 5 delves into an analysis of EU regulatory regime surrounding healthcare emergencies and the deployment of digital healthcare technologies for the managing of such emergencies. Specifically, the chapter examines the impact of the deployment of digital health technologies at the EU and the Member State levels for the management of the Covid-19 pandemic vis-à-vis such technologies' impact on the fundamental rights of privacy, data protection, and health. In this regard, two case studies are provided, focusing on two different technologies:

1. exposure notification applications; and
2. proofs of vaccinations.

Finally, the chapter concludes with an analysis of the proposed legislation at the European level for the management of public healthcare emergencies, and what impact the Covid-19 pandemic had on the drafting of such legislation.

Chapter 6 moves forward with the analysis of the regulatory regime applicable to digital health technologies considering the future of the regulation of such technologies and its impact on individuals. Chapter 6 scrutinises and examines the current European policy and legislative proposals such as: the initiative for EU Digital Decade 2030, the initiative for European Health Union, the proposal for the European Health Data Space, and the proposal for the regulation of Artificial Intelligence, from the perspective of digital health devices and personal data protection. This Chapter provides an in-depth scrutiny of the future of the regulatory and policy regimes within the Union, particularly considering whether such initiatives contribute towards the strengthening of the rights to privacy, the right to data protection.

Chapter 7 examines the European Union's policies and regulatory measures in cybersecurity and their role in big data and AI-powered digital health technologies. A particular focus is placed on the Cybersecurity Act, cybersecurity standardisation and certification initiatives such as ISO, NIST, and the European Commission Regulation 2021/2282 on Health Technology Assessment. By adopting a healthcare perspective, this chapter stresses how the recent policy developments regulating cybersecurity allow the reconciliation of the benefits of big data and AI in digital health technologies regarding the right to privacy and personal data protection. Specifically, the chapter examines how standardisation and certifications can be used as supportive mechanisms not only to ensure regulatory compliance but also to ensure preservation of privacy in digital health technologies without hindering the right to health. The chapter then moves on to the examination of the chosen ISO 27000 family standard analysis and the GDPR specific standard analysis, namely the ISDP 10003, arguing that the application of such standards enhances privacy and personal data protection in digital health technology scenario. This part of the thesis analyses a case study of AI health data management system development, based on research collaboration between public and private entities in the Piedmont region. This analysis is a result of a 6-month internship at a company at the end of the Ph.D. programme. This chapter concludes with an opinion that considering the risk to privacy and data protection of the technological advancements in digital health technologies, third party certifications and standardisation could facilitate better compliance with the existing privacy and data protection laws.

Chapter 8 concludes the thesis, outlining the findings of the analyses carried out in the previous chapters. The conclusion does not attempt to present a complete framework for regulatory solutions in big data and digital health technologies from the perspective of privacy, data protection, and the

right to health. Rather, this chapter insists on the possible changes and areas within the regulatory framework that should be addressed. The normative background that was detailed in the thesis showcases that there are no simple solutions to the issues raised by the current practice. No single blueprint exists for determining how to ensure the fundamental rights to privacy and data protection. Even more, deciding whether the protection is adequate and balanced against other fundamental rights is not easy, even with the available court practice in place.

3 Understanding Big data, Health Technologies, and Healthcare Emergencies

3.1 Introduction to Big data and its Attributes

The notion of big data rarely catches the eye of a philosopher or appears in philosophy science works on how big data should be defined[23]. Yet, in the technical science field, the term itself appeared as early as 1997 as a consequence of research concerning a limited memory of data processing for NASA purposes[24]. While the notion of big data has been discussed in both legal and technical research, to date, no single definition of the notion exists. Some authors have argued that the term big data definition should focus on the 3Vs: volume, velocity, and variety[25,26]. Others also note that the term big data should not focus on attributes of big data such as volume, but rather on the wide range of computational methods that are used to analyse big data sets[27,28,29].

In practice, big data is also a notion associated with the fast-paced technological advancements of the last 15 years or so. Consulting firm Gartner[30] popularised the term, by including it in the industry's well-renowned Gartner's Hype Cycle for Emerging Technologies. The said consulting firm named big data the "Technology Trigger" with 2-to-5-year expectations for mainstream adoption in 2011[31]. In 2013, the term big data was listed as the technology that was near its "Peak of Inflated Expectations" by the consulting firm[32]. In 2014, big data was listed as a technology "Trough of Disillusionment" and in 2015 it disappeared from Gartner's Hype Cycles for Emerging technologies[33,34]. The reason for such fading is not because it reached its "Plateau of Productivity"

---

[23] John Symons and Ramón Alvarado, 'Can We Trust Big data? Applying Philosophy of Science to Software' (2016) 3 Big data and Society.

[24] Michael Cox and David Ellsworth, 'Application-Controlled Demand Paging for out-of-Core Visualization' [1997] Proceedings of the IEEE Visualization Conference 235.

[25] 'Laney, D. (2001) 3D Data Management Controlling Data Volume, Velocity and Variety. META Group Research Note, 6. - References - Scientific Research Publishing' <https://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/ReferencesPapers.aspx?ReferenceID=1611280> accessed 25 November 2021.

[26] Chuck Cartledge, 'How Many Vs Are There in Big data?' 1 <http://www.clc-ent.com/TBDE/Docs/vs.pdf>.

[27] Rob Kitchin, *The Data Revolution : Big data, Open Data, Data Infrastructures & Their Consequences*.

[28] Danah Boyd and Kate Crawford, 'Critical Questions for Big data: Provocations for a Cultural, Technological, and Scholarly Phenomenon' (2012) 15 https://doi-org.proxy.bnl.lu/10.1080/1369118X.2012.678878 662 <https://www-tandfonline-com.proxy.bnl.lu/doi/abs/10.1080/1369118X.2012.678878> accessed 1 December 2021.

[29] 'The Pathologies of Big Data'.

[30] Douglas Laney is also a former Gartner associate (a VP and Distinguished Analyst with Gartner's Chief Data Officer Research team)

[31] 'Hype Cycle for Emerging Technologies, 2011' <https://www.gartner.com/en/documents/1754719/hype-cycle-for-emerging-technologies-2011> accessed 25 November 2021.

[32] 'Hype Cycle for Emerging Technologies, 2013' <https://www.gartner.com/en/documents/2571624/hype-cycle-for-emerging-technologies-2013> accessed 25 November 2021.

[33] Gartner, 'Big Data' <https://www.gartner.com/en/information-technology/glossary/big-data> accessed 29 October 2019.

[34] 'Gartner Hype Cycle For Emerging Technologies 2015' <https://www.gartner.com/smarterwithgartner/whats-new-in-gartners-hype-cycle-for-emerging-technologies-2015> accessed 25 November 2021.

or became irrelevant. Rather, Gartner's team consider big data to be a megatrend that touches upon so many aspects of the IoE and IoT hype cycles of various emerging technologies that it forms part of almost all the hype cycles. In other words, big data is what powers digital innovation. Thus, it would not do it justice to keep it in the hype cycle which focuses on precise technologies, as big data is what fuels the emerging technology industry in the first place.

The consulting firm Gartner follows the definition provided by Laney in their understanding of the term big data. The attributes of big data established by Laney in his work define big data as "high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimisation"[35,36]. In the healthcare sector, one could say that big data comprises various types of structured and unstructured data including EHRs, fitness/health-tracking wearable devices generated health-related data, biosensors, clinical devices for monitoring vital sign data, clinical record data, physician's prescription data, medical imaging data, biosensor-generated data and so on.

Nonetheless, it is well established that the term big data carries three fundamental attributes with it, the so-called 3Vs that identify big data: volume, velocity, and variety[37]. The definition provided by the consulting firm Gartner is one of the best-known and mostly widely adopted definitions in the digital technology industry as it encompasses the 3Vs that were established by Laney in his work.

To put it in other words, the definition of big data answers three fundamental questions:

1) Can you find the information that you are looking for? - is what the volume of big data attempts to answer;

2) How accurate or truthful a data set may be? - is the fundamental question that veracity is expected to answer; and lastly

3) Is a picture worth a thousand words? - is what the variety of the notion of big data is all about.

The following sections of this chapter analyse the different attributes of big data, which is then followed by a comparative analysis of the existing definitions of big data in the current state-of-the-art legislation in the European context, from a privacy and data protection perspective. Then, the chapter briefly notes the risks and benefits of big data in the healthcare scenario, focusing on the legal and ethical risks posed by using big data and big data analytics. The chapter then moves on from the notion of big data to the notion of health technology and its relationship to big data. Finally, the chapter analyses the notion of emergency in healthcare and its multi-dimensional

[35] 'Laney, D. (2001) 3D Data Management Controlling Data Volume, Velocity and Variety. META Group Research Note, 6. - References - Scientific Research Publishing' (n 25).

[36] ibid.

[37] ibid.

nature. Consequently, the chapter conceptualises the notions of big data, health technology, and health emergencies for the purposes of the thesis.

3.2 Beyond the 3Vs of Big Data: Value as a Fundamental Attribute

As mentioned in the introduction of this chapter, the notion of big data is often associated with the three core attributes: volume, velocity, and variety. However, some authors have identified other features that are associated with big data. For example, it has been observed that data portability and interconnectivity are as fundamental as the 3Vs and should be associated with the term big data[38]. Undoubtedly, data portability and interconnectivity are of paramount importance in the IoE and the IoT as they bring together data, people, processes, and things in a connected manner, providing more relevant and valuable insights. In fact, data portability has been described as "crucial in the context of big data, where the focus lays on leveraging large volumes of varied data from many sources, considerably beyond organisational boundaries"[39]. Nonetheless, it could be argued that a "4th V" should be added to the currently identified fundamental attributes of big data - value. In other words, the question that the 4th V should ask is: Does a dataset provide answers you are looking for? Value of big data is the attribute that provides an answer to such a question. Still, value should not be considered as a new attribute of big data. It has been acknowledged from time to time in research, but often remains, the "silent attribute" of big data. One may even argue that the value of big data has been "found" by the big-tech companies which first realised and deployed tools to analyse data they collected from customers.

Nonetheless, the 4th V-value, as an attribute of big data, is a little more of an intricate concept. Value is typically quantified through the economic or social impact a certain dataset might create. For instance, value that can be extracted from big data in healthcare could lead to the development of new medicines to treat various diseases, and thus increasing revenue for the pharmaceutical sector. Still, value of big data in the healthcare is also the feature that separates such big data from the ones generated from, for example, social media. Precisely, we refer to the insight and the unexplored knowledge that can be extracted from data pools in healthcare. Big data in healthcare is also invaluable, as the use of it could provide for new alternative routes of treatment of illnesses, prevent the spread of diseases, or predict healthcare emergencies.

At the same time, in the wrong hands, big data could be used to identify or re-identify an individual, for discriminatory profiling, as well as to reinforce social exclusion and stratification.

---

[38] Wendy Arianne Günther and others, 'Debating Big data: A Literature Review on Realizing Value from Big data' (2017) 26 Journal of Strategic Information Systems 191.

[39] ibid.

We should note, however, that value as a notion is subjective in the same way one man's trash may be another's treasure. The same may be applied to big data, which may be worthless to one person or organisation in one context but may be valuable to another person or organisation in a different context.

3.2.1 On the Notion of Big data in the European Healthcare Context

In the following paragraphs of the thesis, we emphasise the analysis of big data, which can be found in the European health context from the perspective of data protection. At the European and the international level, no single definition of big data exists. For instance, during the EU Commission's study in 2016, an expert group defined big data in health as:

"Large routinely or automatically collected datasets, which are electronically captured and stored. It is reusable in the sense of multipurpose data and comprises the fusion and connection of existing databases for the purpose of improving health and health system performance. It does not refer to data collected for a specific study"[40].

The definition is intentionally vague. The Commission does not attempt to define the types of health data or health-related data that should be included in the definition. Rather it focuses on the features of big data in healthcare. These features include:

1. large automatically/routinely collected datasets;
2. electronically captured, reusable data;
3. fusion of the data sets;
4. interconnectivity of the data with existing databases,

all with the purpose of improving health and health system performance[41]. Such a definition is broad enough to capture a wide range of health data sources and data related to health which may require special protection, depending on the specific type of data captured.
Similarly, in 2017 the Council of Europe acknowledged that no single definition of big data exists as the notion depends on a specific discipline[42].

[40] European Commission, 'Study on Big data in Public Health, Telemedicine and Healthcare | Digital Single Market' (2016) <https://ec.europa.eu/digital-single-market/en/news/study-big-data-public-health-telemedicine-and-healthcare> accessed 10 December 2019.
[41] ibid.
[42] Consultative Committee of Convention 108 Council of Europe, 'Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big data' (2017) <moz-extension://94734e33-af11-684c-859d-50cd290941f6/enhanced-reader.html?openApp&pdf=https%3A%2F%2Frm.coe.int%2Ft-pd-2017-1-bigdataguidelines-en%2F16806f06d0> accessed 18 March 2020.

Like the Commission, the Council of Europe (henceforth, the "CoE") focuses on the attributes of big data: volume, velocity, and variety. Interestingly, the CoE notes that:

"In terms of data protection, the main issues do not only concern the volume, velocity, and variety of processed data, but also the analysis of the data using software to extract new and predictive knowledge for decision-making purposes regarding individuals and groups. For the purposes of these Guidelines, the definition of big data therefore encompasses both big data and big data analytics"[43].

In the same vein, an advisory body of the EU, the Working Party 29 (henceforth, the "WP29") has given its opinion about the term big data. According to WP29, big data refers to the:

"Exponential growth both in the availability and in the automated use of information: it refers to gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed (hence the name: analytics) using computer algorithms. Big data can be used to identify more general trends and correlations, but it can also be processed to directly affect individuals"[44].

Big data thus can be described as "a shorthand for the gathering, analysis, processing, and use of immense exploitable datasets, including both structured and unstructured digital information, that has become one of the compelling causes of data-driven businesses and innovations"[45].
The newest regulatory proposals in the EU do not shed further light on the clear understanding of big data in the context of healthcare. For example, the proposal for the regulation on the European Health Data Space (henceforth, the "EHDS"), that proposes the creation of a single interoperable European Health Data Space for the exchange of healthcare records, mentions big data only once in its explanatory note. The EHDS proposal stresses the non-binding nature of European documents on big data that were not followed up by "further specific actions and their implementation in practice remains very limited"[46]. Likewise, the text of the EHDS proposal itself only refers to notions such as personal electronic health data, non-personal electronic health data, or electronic health data which simply refers to both types of data, giving no further clarification on big data in healthcare.

[43] ibid.
[44] Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (2013) <http://ec.europa.eu/justice/data-protection/index_en.htm> accessed 14 December 2020.
[45] / Anr and others, 'Personal and Non-Personal Data in the Context of Big data' (2017).
[46] Proposal for a Reglation of the European Parliament and the Council on the European Health Data Space COM(2022) 197 final.

While a single definition of big data in healthcare may not exist at the EU level, a general definition of was provided in the European policy for shaping Europe's digital future. The policy document refers to big data as "large amounts of data produced very quickly by a high number of diverse sources. Data can either be created by people or generated by machines, such as sensors gathering climate information, satellite imagery, digital pictures and videos, purchase transaction records, or GPS signals"[47]. The notion further refers to data value chain whereas value in the data sets can be generated at different stages and may bring opportunities and provide valuable insight for several sectors.

3.2.1.1 Observations on Big data in the European Privacy and Data Protection Context

In the field of privacy and data protection, we examine the definition of big data as well. Interestingly, the GDPR, being the cornerstone of the EU's data protection laws, does not define big data nor big data in healthcare. Instead, the approach taken in the GDPR focuses only on defining specific categories (types) of data. In this regard, Article 4(1)(a) defines personal data as:

"data which as 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 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"[48].

Furthermore, Article 4 provides a definition of data concerning health which is defined as "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"[49]. Similarly, the GDPR Article 4 also includes the definitions of genetic data and biometric data[50,51].

---

[47] 'Big data | Shaping Europe's Digital Future' <https://ec.europa.eu/digital-single-market/en/big-data> accessed 30 June 2020.

[48] The European Parliament and The Council Regulation (EU) 2016/679 of the European Parliament and 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 (n 9).

[49] Nicholas Vollmer, 'Article 4 EU General Data Protection Regulation (EU-GDPR)' <http://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm> accessed 12 November 2019.

[50] Under Article 4 of the GDPR "genetic data" means "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."

[51] Under Article 4 of the GDPR "biometric data" means "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."

Furthermore, the GDPR recognises data concerning health as a special category of data. The preamble's paragraphs reaffirm the same and, paragraph 53 of the recital notes that such special categories of personal data merit "higher protection"[52] and should be "processed for health-related purposes"[53] provided that these purposes benefit natural persons or society. Also, Recital 54 also that processing without consent of the "special categories of data" may be permitted only when the purpose of the processing is public interest or public health.

In respect of data concerning health, Article 9 of the GDPR provides a data protection regime applicable to the special categories of data. It also provides guidance on how to handle such data.

The regulatory regime established by the GDPR, which focuses on the types of data requiring protection, introduces a broad scope of what can be understood as a notion of big data in healthcare. Thus it could be argued that the notion includes all information related to an individual's health, genetic data, biometric data, and includes any personal health data that may be extracted from big data sets.

In 2019, the Council of Europe issued Guidelines Regarding Processing of Health-Related Personal Data for GDPR purposes, outlining the principles such processing should follow. In fact, the Council of Europe defined health-related data as "all personal data concerning the physical or mental health of an individual, including the provision of health-care services, which reveals information about this individual's past, current and future health"[54]. The definition used in the guidelines seems to expand the scope of data protected through the inclusion of the "past, current, and future personal health data and health related datasets"[55]. The further elaboration by CoE regarding the concept of personal data related to health and health-related data suggests that "the protection of big data in healthcare does not only include personal healthcare records but expands to all types of data that can indicate an individual's health status and thus, requires special protection"[56].

Also, this dichotomy between the term big data used in the IT industry and the terminology used by the legislators in the EU is what brought to question whether the GDPR's approach to data protection in the age of big data will be capable of addressing the risks and keep up with the technological advancements[57].

---

[52] The European Parliament and The Council Regulation (EU) 2016/679 of the European Parliament and 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 (n 9).

[53] ibid.

[54] Aiste Gerybaite and Paola Aurucci, 'Big data and Pandemics: How to Strike in the Age of GDPR' [2020] Intelligent Environments 2020: Workshop Proceedings of the 16th International Conference on Intelligent Environments 115.

[55] Trix Mulder, 'The Role of Law in Protecting Personal Data Generated by Health Apps and Wearables' (University of Groningen 2022).

[56] Gerybaite and Aurucci (n 54).

[57] Bart Van der Sloot and Aviva De Groot, *The Handbook of Privacy Studies: An Interdisciplinary Introduction*

From the various interpretations provided with respect to the notion of big data and considering the fundamental attributes of big data we can draw a handful of conclusions. Before all else, the value of big data is often seen as a consequence of its analysis, for example, when big data analytic tools are employed. Big data is not often considered valuable per se, i.e., in its initial state, before any analysis on the data set is done. Conversely, when assessing the non-provision of the definition of big data in the GDPR and the CoE guidelines on health-related data, it can be observed that both take a fundamentally different approach to big data. The GDPR, and in turn the CoE, take the stance that big data, in the context of GDPR personal and personal sensitive data, is value per se, in its initial state, whether in a big data set or not, and since (personal) data is value, it requires protection in the digital world.

Also, the portability and interoperability aspects of big data are only directly addressed in two out of six analysed definitions. The interoperability and data portability in the IoT and IoE add an additional layer of complexity. Data interoperability, also addressed by the EHDS, and data portability allow data collected from various devices such as smart watches, health devices, patient records to be combined and analysed together for further insight and decision making.

Lastly, we can observe that there is no common definition of big data, as defining big data could entail a requirement for the protection of big data per se at a regulatory level, whether these are personal or non-personal data. Yet, the more intertwined our lives are with technologies, the more data we put into the digital space, the more accurate data analytics becomes in terms of not only predicting individual preferences, but also future choices, and the more data may affect those falling within the same or similar categories. Thus, questioning the very predicament of the protection of only personal data and not data on a broader scale.

3.2.2 On Big Data-Driven Healthcare: The Advantages and Risks of Big Data

Big data plays an integral part of this digitisation effort and has changed the way we understand both public and individual healthcare. The healthcare industry's widespread digitisation efforts in Europe, together with changing business models, are changing the needs of the patients and are reshaping healthcare economy[58].

In this respect, big data has brought basic benefits such as improved sharing of medical data which includes electronic health records, reduction of duplicate procedures, such as tests being ordered by

(Amsterdam University Press 2018) <https://www.aup.nl/en/book/9789462988095/the-handbook-of-privacy-studies> accessed 16 January 2020.

[58] David Gotz and David Borland, 'Data-Driven Healthcare: Challenges and Opportunities for Interactive Visualization' (2016) 36 IEEE Computer Graphics and Applications 90.

medical professionals, or streamlining hospital administrative procedures and allowing medical practitioners to focus on the patient and provide a more patient-centred healthcare.

Yet, big data has also gone beyond the basic benefits it can provide in healthcare. The healthcare industry has recognised the inevitable application of big data to enable data-driven decision assistance in decision-making for health practitioners, data-driven learning healthcare systems, and personalised treatment plans.

In the healthcare emergencies domain, big data has a few, more particular advantages: prevention[59], detection[60], monitoring[61]. Regarding prevention, big data analytics has already showed that it can prevent mass diseases by detecting diseases in their early stages and then by modelling the spread of infection such as in the case of the Covid-19 pandemic[62]. Also, big data analytics can detect and forecast change in a patient's vital signs through real-time monitoring, leading to on-time intervention and prevention of unneeded emergency room visits[63].

In the same way that big data analytics provides benefits to the healthcare industry, it also poses risks, since data builds on data. The more data is collected and processed, the more accurate data analytics become and allow us to build trust on its suggested patterns and observations. These patterns and observations are particularly useful in healthcare, allowing medical practitioners to deliver better healthcare to patients.

Yet, since data builds on data, the many benefits of big data analytics in healthcare can sometimes be outweighed not only by the risks associated with the technical abilities of data analytics, but also by the risks associated with the data itself.

Risks associated with big data in healthcare can be divided into two broad categories: legal and ethical risks, and technical risks. From the technical perspective the major risks are associated with security and privacy of data, specifically the protection of personal data or the available tools for the processing of the increased amounts of data.

On the latter, we refer to ethical and legal risks of big data in healthcare. With respect to data ethics, we should note that "data ethics focuses on ethical problems posed by the collection and analysis of large"[64] datasets. These risks range from the use of big data in various scenarios, such as healthcare.

---

[59] Efrat Shadmi and others, 'Predicting 30-Day Readmissions with Preadmission Electronic Health Record Data' (2015) 53 Medical care 283 <https://pubmed.ncbi.nlm.nih.gov/25634089/> accessed 8 November 2021.

[60] M Dion, P AbdelMalik and A Mawudeku, 'Big data and the Global Public Health Intelligence Network (GPHIN)' (2015) 41 Canada Communicable Disease Report 209.

[61] Javier Andreu-Perez and others, 'Big data for Health' (2015) 19 IEEE Journal of Biomedical and Health Informatics 1193.

[62] Effy Vayena and others, 'Digital Tools against COVID-19: Taxonomy, Ethical Challenges, and Navigation Aid' (2020) 2 The Lancet Digital Health e425 <www.thelancet.com/digital-health> accessed 28 October 2020.

[63] Sadia Din and Anand Paul, 'Erratum to "Smart Health Monitoring and Management System: Toward Autonomous Wearable Sensing for Internet of Things Using Big data Analytics [Future Gener. Comput. Syst. 91 (2019) 611–619]" (Future Generation Computer Systems (2019) 91 (611–619), (S01677' 1350.

[64] Luciano Floridi and Mariarosaria Taddeo, 'What Is Data Ethics?' (2016) 374 Philosophical Transactions of the Royal

For example, some authors observe ethical challenges in big data in public healthcare, such as healthcare data's context sensitivity[65]. Take, for example, digital epidemiology which is a public health function aiming at improving health of the public at large. Such an aim could be considered a common good, also benefitting individual members of societies, whereas commercial activities using the same big data have a contrasting goal of economic profitability[66]. This entails the ethical obligations in these two scenarios being different, as one use of big data may not be acceptable for commercial entities but encouraged in the public sector[67]. If we were to extend the same digital epidemiology example to the Covid-19 scenario, ethical risks related to trust and transparency of big data can be observed[68].

Other ethical risks observed by authors refer to the methodological robustness of big data analytics whereas incomplete or deficient methodologies may harm individuals, communities, or businesses due to false results[69]. Additionally, some also note that a key concern of big data ethics is the possibility of re-identification of individuals through big data mining activities (arguably, more a legal risk rather than an ethical one) and risks associated to the so-called "group privacy"[70,71].

These ethical risks can often transpose into legal risks. Consider the same example of the digital epidemiology mentioned above. When there is a lack of methodological robustness on big data analytics and protection of personal data in a commercial setup, individuals may suffer from unjustified exposure of personal data or financial losses, to give a few examples. In the same way, the so-called group-privacy ethical concerns may lead to legal risks such as stigmatisation or discrimination of a particular community. For example, by falsely identifying a particular community as an outbreak of a disease.

In addition, both individuals and groups may suffer from restrictions to freedoms, such as the ones enshrined in the Treaty of the European Union (henceforth, the "TEU") and the Treaty on the Functioning of the European Union (henceforth, the "TFEU"), for example, the right of free movement as observed in the Covid-19 example.

While legal risks may take diverse shapes in the digital health industry, the risk to the right to privacy and to data protection could be argued to be the two most pressing ones. Some authors have

---

Society A: Mathematical, Physical and Engineering Sciences 20160360 <https://royalsocietypublishing.org/doi/10.1098/rsta.2016.0360> accessed 26 May 2020.

[65] Vayena and others (n 62).

[66] ibid.

[67] ibid.

[68] Laura S Rozek and others, 'Understanding Vaccine Hesitancy in the Context of COVID-19: The Role of Trust and Confidence in a Seventeen-Country Survey' (2021) 66 International Journal of Public Health.

[69] Urs Gasser and others, 'Digital Tools against COVID-19: Taxonomy, Ethical Challenges, and Navigation Aid' (2020) 2 The Lancet Digital Health e425 <www.thelancet.com/digital-health> accessed 27 October 2020.

[70] Floridi and Taddeo (n 64).

[71] U Pagallo, 'The Collective Dimensions of Privacy in the Information Era: A Comparative Law Approach' (2020) XI Annuario di diritto comparato e di studi legislativi 115.

long (long before the GDPR came into force) questioned whether methods such as de-identification are sufficient to protect personal health data[72]. These rights form part of the basis of fundamental rights of the EU, which are protected under the Charter of Fundamental Rights of the European Union (henceforth, "CFR") Articles 7 and 8. The said articles enshrine the right to privacy and the right to data protection, respectively. Therefore, further sections of this work will analyse various approaches to ensuring the above-mentioned rights against the right to health in selected healthcare scenarios.

Finally, it is nearly impossible to establish all the ways in which big data is changing and will change the healthcare industry in the future - the only limit is the data analyst's imagination. Yet, we should make one final observation: big data healthcare analytics may one day lead to having predictable health. A healthcare system so advanced where a patient's health can be reasonably predicted using big data analytics tools. A healthcare system where patients will be aware in advance of the potential health hazards and ways to prevent or treat them, and benefits to all stakeholders involved.

3.3 On the Notion of Digital Health Technologies

In studies about various digital health technologies, it is typical to find work that addresses privacy and cybersecurity aspects[73]. Still, little work may be found in addressing what are considered as digital health technologies.

The term health technology itself predates the digital era and health information technology. Health technologies in the predigital age referred to such organised knowledge and skills that allowed to alleviate a health problem or improve healthcare quality. For example, simple, hand-written patient health records in the pre-digital era which were kept in a centralised location at a hospital and included all history of a particular patient, predate health technology. With information technologies spreading into various sectors, these patient health records moved from paper format into digital format, and were saved on a hospital's servers, cloud, or even patient's devices. In a sense, the digitalisation efforts have further improved existing health technologies, and, also, digitalisation has found new ways to improve healthcare.

In the research world, there is little common understanding of what digital health technologies are, often focusing on technologies and way to manage risks of such technologies. Much of the research

[72] Mark A Rothstein, 'Is Deidentification Sufficient to Protect Health Privacy in Research?' (2010) 10 The American Journal of Bioethics 3 <http://www.tandfonline.com/doi/abs/10.1080/15265161.2010.494215> accessed 19 March 2020.

[73] Aiste Gerybaite, 'Digital Governance: The Case of Proofs of Vaccination' [2021] ACM International Conference Proceeding Series 450.

is focused on creating mechanisms to protect privacy and data in digital health technologies. For example, in the context of privacy modelling, research focus lays with modelling privacy requirements for mHealth applications, such as pseudonymity of patients, data minimisation and transparency in goal management training applications[74]. Other authors discuss how blockchain enabled frameworks for mHealth could deal with the arising privacy issues and propose the use of a private blockchain based on the Ethereum platform, where wearable sensors can communicate with a smart device that uses a peer-to-peer hypermedia protocol, the InterPlanetary File System[75]. Similarly, Atarian et al. propose an anonymous protocol for protecting mHealth data via the blockchain smart contracts and Elliptic Curve Cryptographic solutions which enable mHealth transactions to be implemented in a distributed and trusted way[76]. Other studies focus on taxonomies for privacy governance in health IoE. For instance, IoE has been proposed in a purposed-based taxonomy for better governance of personal data in health[77].

Besides, other academic research shifts from technical solutions to improve privacy and data protection to addressing legal risks associated with regulated medical devices. For example, addressing the eHealth Platform as a Service (henceforth, the "PaaS") for consumer mHealth in light of the EU's Medical Device Regulation (henceforth, the "MDR"). Research on this has observed that the PaaS undermines legal compliance and the MDR[78] and will remain a grey area ridden with legal uncertainty[79]. Also, Sheppard finds that mHealth applications are greatly dependent on patient trust in the safety and security of the new technologies[80].

Similarly, in the light of stand-alone software as a medical device, several contributions have been made by the Court of Justice of the European Union (henceforth, the "CJEU") case law (for example, the Snitem ruling (C-329/16)), where the analysis is heading towards the needed debate for an updated regulatory framework for medical artificial intelligence and big data[81].

---

[74] Alexander Gabel and others, 'MHealth Applications for Goal Management Training - Privacy Engineering in Neuropsychological Studies' (2018) 526 IFIP Advances in Information and Communication Technology 330.

[75] Dragos Daniel Taralunga and Bogdan Cristian Florea, 'A Blockchain-Enabled Framework for Mhealth Systems' (2021) 21 Sensors.

[76] Reyhane Attarian and Sattar Hashemi, 'An Anonymity Communication Protocol for Security and Privacy of Clients in IoT-Based Mobile Health Transactions' (2021) 190 Computer Networks 107976.

[77] Claire Levallois-Barth and Hugo Zylberberg, 'A Purpose-Based Taxonomy for Better Governance of Personal Data in the Internet of Things Era: The Example of Wellness Data' 139.

[78] Medical Device Regulation

[79] Nadezhda Purtova, 'EHealth Spare Parts as a Service: Modular EHealth Solutions and Medical Device Reform' (2017) 24 European Journal of Health Law 463 <http://catalogue.fi-star.eu/> accessed 26 October 2020.

[80] Maria K Sheppard, 'MHealth Apps: Disruptive Innovation, Regulation, and Trust — A Need for Balance' (2020) 28 Medical Law Review 549.

[81] Timo Minssen, Marc Mimler and Vivian Mak, 'When Does Stand-Alone Software Qualify as a Medical Device in the European Union? — The CJEU's Decision in Snitem and What It Implies for the next Generation of Medical Devices' (2020) 28 Medical Law Review 615 <https://academic.oup.com/medlaw/article/28/3/615/5865470> accessed 7 June 2021.

Lastly, research also focuses on the cybersecurity aspects of digital health technologies. For example, Maccioni et al. address the need for cybersecurity expansion for applications with a medical purpose which fall in the grey area and are not covered under the MDR[82]. In this respect they note that the concept of safety must be understood with a different and broader meaning[83]. It can be observed from the above that the research focuses on different aspects of digital health technologies, be it mHealth devices or eHealth platforms.

In addition, it could also be noted that scientific work often focuses on how health technologies or digital health technologies (the terms are often used interchangeably) can improve healthcare, and little on what is considered health technology or as a digital health technology for ethical, legal, and regulatory purposes. For this reason, we conceptualise the notion of digital health technology used in this thesis.

In EU legislation we may find several definitions of digital health technologies, varying from medicinal products, medical devices, to health technology itself. We start our analysis of the notion health technology from a rather unusual place, by taking an analytical view of the medicinal products directive[84] and the definitions therein. The said directive refers to medicinal products as "any substance or combination of substances presented for treating or preventing disease in human beings"[85]. At a first glance, it could appear that medicinal products would fall outside the scope of a notion of health technology as one could mistakenly assume that medicinal products are primarily pharmaceuticals.

Yet, the medicinal products directive deals with use and administration of various substances, irrespective of their origin, which may be administered to humans for health purposes, be it for restoring or correcting physiological functions or making a medical diagnosis[86]. In recent years, the use of the so-called "smart pill" has been discussed extensively in research, as such tiny capsule-like hybrid device/medicinal products could incrementally aid healthcare, both for medical diagnosis and ensuring patience medicine intake at the right time and right dosages[87,88]. A smart pill

---

[82] Giovanni Maccioni and Daniele Giansanti, 'Medical Apps and the Gray Zone in the Covid-19 Era: Between Evidence and New Needs for Cybersecurity Expansion' (2021) 9 Healthcare (Switzerland) 430 <https://www.mdpi.com/2227-9032/9/4/430/htm> accessed 9 June 2021.

[83] ibid.

[84] European Parliament, Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use 2001 67.

[85] ibid.

[86] ibid.

[87] Rosa Goffredo, Dino Accoto and Eugenio Guglielmelli, 'Swallowable Smart Pills for Local Drug Delivery: Present Status and Future Perspectives' (2015) 12 http://dx.doi.org.proxy.bnl.lu/10.1586/17434440.2015.1061933 585 <https://www-tandfonline-com.proxy.bnl.lu/doi/abs/10.1586/17434440.2015.1061933> accessed 29 November 2021.

[88] Craig M Klugman and others, 'The Ethics of Smart Pills and Self-Acting Devices: Autonomy, Truth-Telling, and Trust at the Dawn of Digital Medicine' (2018) 18 https://doi-org.proxy.bnl.lu/10.1080/15265161.2018.1498933 38 <https://www-tandfonline-com.proxy.bnl.lu/doi/abs/10.1080/15265161.2018.1498933> accessed 29 November

could both be considered a medicinal product and a digital health technology, with the line between the two being very blurred, considering the lack of a common definition of a digital health technology.
Medical devices, on the other hand, are defined by the MDR, and are considered to include:

"Such devices and instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more specific medical purposes and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means"[89].

The definition of medical devices is limited to such that are intended by the manufacturer of the device to be marketed as a medical device and undergo the necessary authorisation mechanism established under the MDR. Thus, various health-related applications that, for instance, may be found on Google Play or Apple Store, are not necessarily medical devices, even though they may be used to assess one's general health. The two above-mentioned legislative attempts do not define digital health technologies per se, however, they both define a certain type of health technology.
One can also locate the term health technology defined in other European legislative attempts in the healthcare sector. In this respect, for example, the EU Patient's Rights Directive, which protects patients' rights, also addresses the notion of health technology. In the context of the EU Patient's Rights Directive, health technology is defined "as a medicinal product, a medical device, or medical and surgical procedures as well as measures for disease prevention, diagnosis or treatment used in [healthcare]"[90]. Similarly to the MDR, the Directive on Patient Rights also excludes from the notion of health technology any health-related applications that do not undergo an authorisation process but nevertheless may have an impact on the health of individuals, such as the Covid-19 applications or fitness trackers.
Finally, on the global scale, the World Health Organisation (WHO) provides a definition of health technology, which perhaps is the most accurate for this thesis. In the resolution adopted by the Sixtieth World Health Assembly in 2015, the WHO observed that the term health technology refers to "the application of organised knowledge and skills in the form of devices, medicines, vaccines,

---

2021.

[89] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EE 2017.

[90] OJ L 88 European Parliament, Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare 2011 45.

procedures and systems developed to solve a health problem and improve quality of lives"[91]. Therefore, digital health technologies should be considered as an umbrella term that incorporates all types of digital instruments that can be deployed in the healthcare context. Considering the scope of this thesis, which explores and analyses the multi-dimensional nature of digital healthcare technologies for emergencies, the WHO's definition encompasses the wide range of such technologies.

3.3.1 A Taxonomy of Digital Health Technologies for Health Emergencies

The stimulus for incentivising the use of digital health technologies is unmistakable, as the revenue for health technology in 2022 should grow to 6.1 billion U.S. dollars[92]. Such vast market growth has proved that devices that monitor heart rate, glucose levels, sleeping patterns, or amounts of physical activity are now essential tools in the digital society. Similarly, vital sign monitoring devices which send emergency signals to healthcare professionals are now essential in the digital world and have been applied in various scenarios, especially involving elderly people.

Current research has focused on developing tools and applications which, for instance, track elderly people within their home environments and detect falls, which may be fatal[93]. Such technology can be highly invasive as it provides real-time surveillance of an individual and thus threatens a person's privacy by affecting data protection if the tools are not designed with the highest data protection and security standards.

Also, with the outbreak of the Covid-19 pandemic in early 2020 in Europe, we witnessed the rise of other types of digital healthcare technologies such as contact tracing, symptom tracking, geo-localisation, quarantine applications (surveillance tools for individuals in quarantine, mostly used by law enforcement), or the so-called immunity passports which were assisting countries to manage the Covid-19 emergency. Some of these technologies, such as contact tracing applications which use a GPS signal to track individuals have brought about some concerns regarding unauthorised surveillance and potential breaches of data protection and privacy, especially in the EU. Such technologies combined with personal healthcare monitoring devices such as ECG, glucose monitoring devices, or in-vitro devices such as pacemakers collect and process unprecedented amounts of potentially sensitive data which ought to be protected.

---

[91] WHO, Resolution on Health Technologies 2015.

[92] 'Global AI Market for Healthcare Applications 2018 and 2022 | Statista' <https://www.statista.com/statistics/743877/worldwide-artificial-intelligence-market-healthcare-application/> accessed 13 October 2020.

[93] Sumit Majumder and others, 'Smart Homes for Elderly Healthcare—Recent Advances and Research Challenges' (2017) 17 Sensors (Basel).

Health technologies in emergency healthcare may also be considered as an umbrella term for all digital health technologies that assist, either directly or indirectly, with the management of personal and public health emergencies, and technologies that predict or prevent health emergencies. Such technologies often use systems which allow, for example, tracking of vital signs, sending emergency signals in cases of accidents or tools that assist in managing public healthcare emergencies as mentioned above.

To date, research has focused on the development of such systems that may be generally classified into:

1. Intelligent Emergency Response Systems[94]. Such technologies use improved IT systems to manage emergency calls and vehicles and manage incidents[95]. For instance, research projects based in the Italian regions of Piedmont and Lombardy focused on the dispatching of ambulances in emergency situations[96],.

   With the shift of the healthcare systems that focus on the services providers to healthcare services focused on the patients, countries around the globe have been re-inventing their approaches to emergency response. Denmark has undergone a shift in the whole emergency response system and now uses a criterion-based decision support tool which determines the urgency of the medical problem rather than having healthcare personnel assign diagnosis over the phone[97]. Also, since the Danish healthcare system assigns a unique registration number to each patient, this allows for conducting high-quality research of a patient in the Danish healthcare registries. Lastly, one of China's regions has revamped their emergency response systems with 5G, by transforming emergency vehicles into mobile emergency centres aided by 5G which allows paramedics to check a patient's vital signs, perform tests from inside the vehicle, and send all such information to the emergency room doctor for guidance in real time[98].
2. Health Monitoring Technologies. Such technologies are often used for personal healthcare and emergency management and "involve measuring and transmitting multiple vital signs and biomedical parameters of the patient to healthcare professionals who then make

[94] Upkar Varshney, Robert Nickerson and Jan Muntermann, 'Taxonomy Development in Health-IT' [2013] AMCIS 2013 Proceedings <https://aisel.aisnet.org/amcis2013/HealthInformation/GeneralPresentations/15> accessed 29 July 2022.

[95] ibid.

[96] Roberto Aringhieri and others, 'Evaluating the Dispatching Policies for a Regional Network of Emergency Departments Exploiting Health Care Big data' (Springer, Cham 2018) <http://link.springer.com/10.1007/978-3-319-72926-8_46> accessed 31 October 2019.

[97] Tim Alex Lindskou and others, 'The Danish Prehospital Emergency Healthcare System and Research Possibilities'.

[98] '5G-Enabled Smart Healthcare Services Make a Huge Difference in Our Lives: No More "Getting There Too Late" | Light Reading' <https://www.lightreading.com/5g-enabled-smart-healthcare-services-make-a-huge-difference-in-our-lives-no-more-getting-there-too-late/a/d-id/753363> accessed 13 January 2020.

healthcare decisions"[99]. In more advanced applications, such a decision may be automated with no or minimal human interaction. In other words, digital health monitoring technologies for healthcare emergencies focus on vital and non-vital sign monitoring. Since this work deals with healthcare emergencies, we establish a premise for the purpose of the research that health monitoring technologies include:

a. Monitoring and tracking of vital signs or other body measurements of patients. In health, vital signs are signs that indicate the status of the body's vital or life-sustaining functions and usually includes body temperature, pulse, respiration rate, and blood pressure. Other signs or body measurements of patients may include a patient's height, weight, body mass index, menstrual cycle, oxygen saturation, blood glucose level, fall detection or even pain. The main differentiation between vital signs and other body measurements are its potential impact on a person's health. Vital signs may indicate acute changes to the person's physical status while other body measurements are not useful for assessing acute changes, however, their measurements are nevertheless important as they allow the impact of chronic diseases or prolonged illnesses on the patient's body to be assessed. The vital signs and other body measurements may be tracked remotely (from home) and either periodically or real-time.

b. Can be worn by a user or patient. The definition of wearable device may be traced back to as early as 1600s, yet the modern understanding of the wearable device dates back to the 1960s when they were known as "wearable computing". Wearable computing was introduced by Thorp and Shannon when they presented a concealed cigarette-pack sized analogue computer designed to predict roulette wheels to help win at roulette. By some authors this is not considered a wearable device but rather as task-specific hardware.

   A more generally purposed wearable device came to light in 1980s with the design of general-purpose wearable computers by Mann, known as the father of wearable computing[100]. After that, wearable computing exploded into all industries of consumer electronics. In the broadest sense wearable devices may be understood as a new manifestation of accessories that people wear, which may be embedded in clothing, implanted in a person's body, or even tattooed on the skin. A similar

[99] Varshney, Nickerson and Muntermann (n 94).

[100] *Wearable Computing | The Encyclopedia of Human-Computer Interaction, 2nd Ed.* <https://www.interaction-design.org/literature/book/the-encyclopedia-of-human-computer-interaction-2nd-ed/wearable-computing> accessed 11 March 2021.

definition of wearables was discussed also by the EU Commission in its 2015 report on smart wearables[101]. In terms of health-related wearable devices, such devices may be:

i. invasive (medical) devices such as pacemakers; and

ii. non-invasive (medical) devices that monitor vital signs and other body measurements.

The distinction between invasive and non-invasive wearables is also the approach taken by the EU MDR as invasive and non-invasive wearables would have diverse health implications on the patient, different security (manufacturing) requirements and, may have different data protection and ethical implications in this respect as well. We must note here that wearables, both invasive and non-invasive, may be considered as medical devices (especially in the case of use of algorithmic software) in terms of the EU Medical Device Regulation.

Often, such health monitoring tools have access to the patient's location to determine if some sort of emergency care is necessary. These technologies are usually used in primary healthcare focusing on the ageing population of the western world and the need of the community care services within the healthcare industry[102]. They include integrating personal healthcare systems for the elderly (such as mobile applications, smartwatches, vital sign monitors and other medical devices) into the general ERS[103]. The amount of healthcare-related data that is collected daily by users of such devices may be found useful for the automated emergency response systems. By pattern-finding algorithms from the big data collected from personal medical devices, emergencies may be detected, and emergency response systems are automatically activated to reach the patient in need. IoE devices used in healthcare may also include fitness/health-tracking wearable devices, biosensors, clinical devices for monitoring vital signs. Such devices generate large quantities of data. If such data is integrated with other existing healthcare data, like healthcare medical records, we may be able to predict patients' health status and its progression from subclinical to pathological state[104]. Data collected from such IoE devices can be greatly advantageous in

[101] Andrew Ruck, 'Information and Stakeholders' Day on Smart Wearables Report' (2015) <http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDo> accessed 11 March 2021.

[102] Randi Stokke, 'The Personal Emergency Response System as a Technology Innovation in Primary Health Care Services: An Integrative Review'.

[103] Hui Ru Cao and Choujun Zhan, 'A Novel Emergency Healthcare System for Elderly Community in Outdoor Environment' (2018) 2018 Wireless Communications and Mobile Computing.

[104] Khader Shameer and others, 'Translational Bioinformatics in the Era of Real-Time Biomedical, Health Care and

offering better investigations and predictions as well as real-time response to emergency situations. A real-time biomedical and health care data stream refers to the compendium of data aggregated by individuals using health-monitoring devices and other health care software systems during ambulatory or inpatient visits that may aid in diagnosis, prognosis, interventions, and stratifications[105].

Also, "Wireless Body Area Network offers a novel prototype for Wireless Sensor Networks in monitoring biomedical sensors"[106], allowing professionals to continuously monitor the health and generate emergency actions in health emergencies. So far, only a few systems cater for the efficient processing of IoE-generated big data[107]. Even fewer of such systems cater for IoE in healthcare generated big data. M. Rathore et al. have implemented a system where the "body readings for each person are transmitted to the Intelligent Building by passing through the Primary Mobile Device (PMD), gateways, and Internet using Bluetooth, ZigBee IEEE 802.15.4, or 3G/LTE/Wi-Fi communication technologies"[108].

3. Digital Health Technologies for public emergencies. These technologies may relate to applications used in cases of natural or "man-made" disasters such as floods, earthquakes, tsunamis, or terrorist attacks (which in turn may impede the health of a population at large) and technologies deployed in cases of tracing various pandemics and viral diseases. These technologies provide support to healthcare authorities and medical staff to provide better response to healthcare. Most of such support technologies for public healthcare emergency management would not require any healthcare professional intervention as they are not based on an individualistic assessment of a patient's situation but are rather focused on supporting national healthcare systems on tracing (e.g., contact) for statistical purposes or for public healthcare policy decision making purposes. Some of these technologies have fallen into the hands of the big-tech companies such as Facebook or Google. For instance, during the 2016 earthquake in the central Apennines of Italy and other various disasters, Facebook provided a "crisis response" technology which allowed people to tag themselves as being safe after the disaster. The same system also aided during hurricane Irma in Puerto Rico in 2017, as it helped individuals seek emergency services by posting on their timelines

---

Wellness Data Streams' (2017) 18 Briefings in Bioinformatics 105 <https://academic.oup.com/bib/article-lookup/doi/10.1093/bib/bbv118> accessed 30 October 2019.

[105] ibid.

[106] M Mazhar Rathore and others, 'Real-Time Medical Emergency Response System: Exploiting IoT and Big data for Public Health' (2016) 40 Journal of Medical Systems 283 <http://link.springer.com/10.1007/s10916-016-0647-6> accessed 31 October 2019.

[107] ibid.

[108] ibid.

and catching the attention of the public and the first responders, as the emergency lines were overflooded.

On the other side of the public healthcare emergencies are the IoT technologies, that are developed to manage various contagious diseases. In fact, contact tracing applications and geo-localisation technologies were used somewhat successfully for combating Zika and SARS viruses in Asia and Africa during 2015 and 2016, and are being used during the ongoing Covid-19 pandemic. Such technologies involved surveillance, contact tracing applications, and other geo-localisation and symptom tracing technologies. The Italian "Immuni" application is one of the examples of the technologies deployed during the Covid-19 pandemic. In fact, one can claim that the success of the application is undoubted from the perspective of data protection and security, as it is one of the first contact tracing apps to be linked via the EU Commission coordinated pan-European system (developed with the Member States and in partnership with German technology companies SAP and Deutsche Telekom) that allowed the applications to "talk" and ensure safer and easier travel within between the EU countries[109].

Whilst both types of research are essential for the healthcare industry, research has not frequently looked at the emergency response system as a whole. In fact, Aringhieri et al. have tried to fill this gap in research with an overview of the full range of the emergency response systems and the future opportunities and challenges within the research area[110]. Aringhieri proposed the development of a system, capable of validating management policies at health system level by modelling the patient flow via the care pathway. With this shift of the healthcare systems from those that focus on the services providers to those healthcare services focused on the patients, countries around the globe have been re-inventing their approaches to emergency response management.

Also, Cao and Zhang have focused on integrating personal healthcare systems for the elderly (such as mobile applications, smart watches, vital sign monitors and other medical devices) into the general emergency response system[111]. The amount of healthcare-related data that is collected daily by users of such devices may be found useful for the automated emergency response systems. By using algorithms that find patterns in the big data collected from personal medical devices, emergencies may be detected, and emergency response systems automatically activated to reach the patient in need.

---

[109] 'Digital Solutions | European Commission' <https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/digital-solutions_en> accessed 15 October 2020.

[110] R Aringhieri and others, 'Emergency Medical Services and beyond: Addressing New Challenges through a Wide Literature Review' (2017) 78 Computers & Operations Research 349 <https://www.sciencedirect.com/science/article/pii/S0305054816302362> accessed 12 December 2019.

[111] Cao and Zhan (n 103).

It may be argued that "linking multiple data sources related to personal or other determinants of health without the individual's informed consent presents a particularly significant privacy risk, especially when the data linkage is not done for the specific purpose of answering a relevant research question or providing a clear public health" benefit. Various authors also argue that while the linkage of data increases the data dimensionality, such dimensionality combined with big data analytic tools, allows "data fingerprints" to be produced, which may allow third parties to re-identify individuals in anonymised data sets through, e.g., deductive disclosure techniques[112].

Interestingly, the OECD report specifies that the use of big data within the public healthcare sector, in a cross-border scenario encounters 4 main challenges: data localisation laws and policies; data security threats that discourage data sharing; lack of global standards for data content and interoperability; and commodification and sale of health data on a world market[113].

In fact, since there are no consistent global standards for content or exchange of such big data, private sectors actors are making business out of it by monetising data.

3.4 On the Notion of Healthcare Emergency: A Multi-Dimensional Nature of Emergency

The protection of life and health are fundamental rights enshrined not only in the Charter of Fundamental Rights of the European Union, but also in national constitutions of the Member States of the EU. These fundamental rights are the basis of legitimisation of any subordinate sources for the protection of such rights permitting both the EU and the Member States implement measures for the protection of such rights.

In the European context, public health is a shared competence of the EU as established in Article 4(2)(k) of the TFEU and is one of the areas where the EU has limited powers. Article 168 of the TFEU, which deals with public health, is the legal basis for most of the EU's initiatives in the healthcare legislation sector. While the aim of the EU is to establish a high level of human health protection, the Union's actions in the healthcare space can only be complementary to national policies. Given that public health is a shared competency of the EU, the possibility of harmonising laws in public health is limited, leading to different approaches to health emergencies and contrasting laws in different Member States.

Thus, defining emergency in healthcare situations from both empirical and legal stand points is a complex matter as it involves many voices and many perspectives. This sub-chapter does not

[112] Stephen J Mooney and Vikas Pejaver, 'Big data in Public Health: Terminology, Machine Learning, and Privacy' (2018) 39 Annual Review of Public Health 95.

[113] *Health in the 21st Century* (OECD 2019) <https://www.oecd-ilibrary.org/social-issues-migration-health/health-in-the-21st-century_e3b23f8e-en> accessed 14 January 2020.

attempt to reinvent the wheel and provide a new definition of emergency in healthcare, rather, it provides a new perspective on healthcare emergencies due to the notion's multidimensional nature.
On the one hand, legal qualifications of emergency may vary from jurisdiction to jurisdiction. On the other side, the empirical understanding of healthcare emergency varies depending on the medical practices within various jurisdictions. For instance, the triage system in the emergency room in the UK is based on clinical assessment by the first attending physician, whilst in the U.S. the nature of an emergency is judged by a patient's initial presentation, rather than an initial diagnosis or suspicion[114].
At the same time, a healthcare emergency, such as an outbreak of a virus, may not necessarily qualify as a health emergency if considered from one individual's perspective (e.g., one that does not live in the affected area). However, it may qualify as a public health emergency if the same virus affects a community at large. For example, SARS or the Covid-19 outbreaks which put almost all the European countries in lockdown conditions.
Furthermore, public health emergencies are typically announced by national governments or international organisations such as the WHO, which is not the case in an individual health emergency. Similarly, a declaration of a healthcare emergency, due to public health concerns, is vital when it comes to authorities being able to activate funds, or personnel to protect public health.
The above examples illustrate that the definition of healthcare emergency depends on the context it is used in, the jurisdiction it occurs in, and the standard medical practices accepted. The above examples also illustrate why the process of defining healthcare emergency can become a contested matter.
In fact, the World Health Organisation defines emergency as a "term describing a state. It is a managerial term, demanding decision, and follow-up in terms of extra-ordinary measures"[115]. It then goes further, explaining the meaning of the state of emergency which:

"Demands to "be declared" or imposed by somebody in authority, who, at a certain moment, will also lift it. Thus, it is usually defined in time and space, it requires threshold values to be recognised, and it implies rules of engagement and an exit strategy. Conceptually, it relates best to response"[116].

[114] Namita Jayaprakash and others, 'Crowding and Delivery of Healthcare in Emergency Departments: The European Perspective.' (2009) 10 The western journal of emergency medicine 233 <http://www.ncbi.nlm.nih.gov/pubmed/20046239> accessed 25 November 2019.
[115] 'WHO | Definitions: Emergencies' [2014] WHO <https://www.who.int/hac/about/definitions/en/> accessed 25 November 2019.
[116] ibid.

What is more, from an empirical point of view, defining emergency in healthcare is problematic as the state of health and health conditions of an individual are dynamic and often change over time. What does not seem to be an emergency may become one as time passes or when certain health conditions change. Notwithstanding such changes, having a common understanding of healthcare emergency is useful to be able to classify health events for purposes of resource allocation, managing risks and even liability.

In the European context, the 2021 proposal for a regulation on Serious Cross-Border Threats to Health, for instance, which aims at extending measures to various public healthcare emergencies, does not use the term healthcare emergency itself. It rather uses the term "serious cross-border threat to health" which, in Article 3(7) of the proposal, is defined as:

"a life-threatening or otherwise serious hazard to health of biological, chemical, environmental, climate or unknown origin which spreads or entails a significant risk of spreading across the national borders of Member States, and which may necessitate coordination at Union level in order to ensure a high level of human health protection"[117].

The above definition reiterates the original definition that was adopted by the EU Parliament and the Council in 2013[118]. A noteworthy aspect of the proposed regulation is that under the new proposal, the Commission will be able to declare a public health emergency at the European level, following a consultation with the Advisory Committee, the WHO, and other related bodies.

Similarly, at the international level, the WHO International Health Regulations do not use the term health emergency, but "public health risk"[119] instead, which is described as "a likelihood of an event that may affect adversely the health of human populations, with an emphasis on one which may spread internationally or may present a serious and direct danger"[120,121].

The Medical Device Regulation follows the same line of thought as the proposal for the regulation on the Serious Cross-Border Threats to Health and does not refer to the term health emergency, but instead uses the same terminology of serious public health threat which is described as:

[117] European Commission Proposal for a Regulation of the European Parliament and the Council on serious cross-border threats to health and repealing Decision No 1082/2013/EU (n 13).

[118] Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC 2013 (OJ L 293) 1.

[119] Antonio Herman Benjamin and others, 'Legal Policy & Pandemics' (2021) 1 The Journal of the Global Pandemic Network.

[120] ibid.

[121] International Health Regulations (2005) 2005 (Lancet) 1249.

"An event which could result in imminent risk of death, serious deterioration in a person's state of health, or serious illness, that may require prompt remedial action, and that may cause significant morbidity or mortality in humans, or that is unusual or unexpected for the given place and time"[122].

The MDR also includes a definition of a serious incident which means:

"any incident that directly or indirectly led, might have led or might lead to any of the following: (a) the death of a patient, user or other person, (b) the temporary or permanent serious deterioration of a patient's, user's or other person's state of health, (c) a serious public health threat"[123].

It should be observed that definitions provided in the MDR and the EU proposal for the regulation on the Serious Cross-Border Threats to Health have different scopes. The proposal on the Serious Cross-Border Threats to Health attempts to deal with public health emergencies, while the MDR focuses on individual health emergencies, including also, a serious public health threat that may become a threat to an individual's health. Both definitions are not mutually exclusive, rather they are inclusive and supplementary to one another.

At the national level, the situation differs significantly. For instance, in the UK, the NHS defines emergency in health as a "life threatening illnesses or accidents which require immediate, intensive treatment. Services that should be accessed in an emergency include ambulance (via 999) and emergency department"[124].

Interestingly, the NHS distinguishes between an emergency and urgency when examining healthcare emergencies. The main difference between the two concepts is that urgent healthcare is not a life-threatening situation, rather a situation that requires urgent attention.

Also, an urgent situation differs from an emergency as it is focused on a phone consultation, pharmacy advice, or out-of-hours general practitioner's appointment. In addition, from an empirical perspective, the NHS employs the triage system, a common practice in the industry. However, this system differs from state to state. In the United Kingdom, for example, the triage system has five national codes for emergencies:

1. "Immediate resuscitation (patients who need immediate treatment for preservation of life).
2. Very urgent (seriously injured/ill whose lives are not in immediate danger).

[122] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EE.

[123] ibid.

[124] 'NHS England » About Urgent and Emergency Care' <https://www.england.nhs.uk/urgent-emergency-care/about-uec/> accessed 11 December 2019.

3. Urgent (patients with serious problems, but apparently stable conditions).
4. Standard (patients without immediate danger or distress).
5. Non-urgent (patients whose conditions are not true accidents or emergencies)[125]".

In Italy, the Italian National Protection Services, the so-called Protezione Civile, defines health risk as:

"The consequence of other risks and calamities, to the point of being defined as a second-degree risk. The health risk factor may be considered as a qualitative variable representing the possibility of an external factor causing harm to the population's health. The probability that this could happen indicates the extent of the risk, i.e., the effect it could cause"[126].

It further provides a non-exhaustive list of examples of risks such as anthropic, e.g., biological nature, such as bacteria, virus, pollens, or natural risks such as earthquakes, floods and so on. Just like the UK's NHS system, the Italian healthcare emergency system also adopts a triage system, composed of four national codes for emergencies:

1 Code red- very critical, life-threatening, highest priority, immediate access to care;
2 Code yellow- medium critical, presence of developmental risk, possibly life-threatening;
3 Code green- not very critical, no developmental risks, deferrable performance;
4 Code white- non-critical, non-urgent patients[127].

The multi-dimensional nature of healthcare emergency explains why in the EU, no single health emergency definition exists, either from a legal or from an empirical perspective.
Finally, we should conclude that healthcare will remain a context-driven notion. If example is taken from the triage systems compared above, the Italian and the UK systems describe different emergency situations purely empirically, which may create legal issues if in practice a healthcare emergency is classified wrongly by medical staff. It is especially relevant in the case of medical professionals' legal liability towards patients.

[125] 'Attribute: A AND E Initial Assessment Triage Category' <https://www.datadictionary.nhs.uk/data_dictionary/attributes/a/a_and_e_initial_assessment_triage_category_de.asp?shownav=1> accessed 18 December 2019.
[126] Protezione Civile, 'Description of the Risk' <http://www.protezionecivile.gov.it/risk-activities/health-risk/description> accessed 17 December 2020.
[127] 'I Codici Colore Gravità (Triage)' <http://www.salute.gov.it/portale/temi/p2_6.jsp?lingua=italiano&id=1052&area=118 Pronto Soccorso&menu=vuoto> accessed 17 December 2020.

Furthermore, when considered in the healthcare innovation context, a study showed that the innovation in healthcare focuses on telehealth, biosensors, wireless trackers, point-of-care diagnostics and so on, while in the so-called healthcare emergencies context the innovation focuses on emergency system management and emergency resource management due to the empirical and multidimensional notion of healthcare emergency[128].

Finally, the multidimensional nature of healthcare emergencies may also create difficulties when applying and developing big data applications for emergency management. For example, a European solution for cardiac arrest monitoring may not take into account the differences in genetics, nutrition, lifestyle, body composition and so on of the various European nations thus providing false or inaccurate results of such life-threatening condition.

3.5 Conclusive Remarks

As the saying goes, extraordinary times call for extraordinary measures. Extraordinary times can be considered as events that change the pace of history due to the event's nature. Be it the change in the course of history due to a political event that, for instance, has ended the Cold War or a terrorist attack, such as 9/11. In cases such as public emergencies and public health emergencies, such extraordinary measures may vary. For instance, in cases of yearly flu outbreaks, governments may increase influenza vaccinations and suggest their citizens take precautionary measures to protect themselves. In more serious health emergencies which, for example, pose a higher risk to the public and individual health and wellbeing, the government's measures may be stricter due to the risk posed. Take, for example, the Covid-19 outbreak in 2020, where national governments worldwide introduced measures ranging from obligatory mask-wearing (most of the EU countries[129]) to lockdowns (Spain, Italy, Lithuania[130]), and obligatory quarantined person tracking (Poland[131]).

Additionally, it should be observed that the state of the Covid-19 crisis presupposes an objective factual situation. Therefore, a declaration of a health emergency by a healthcare function is made on the implied understanding that emergencies are situations of threat, often a great one, that necessitate an urgent response. It can be observed that the common understanding of an emergency is that such emergencies cover man-made events, natural disasters and are often, location-based, i.e., usually, emergencies are localised to one or several geographical areas (for example, in cases of earthquakes). Yet an emergency such as a life-threatening virus transcends borders and

[128] 'Top 10 Health Care Innovations | Deloitte | Center for Health Solutions' <https://www2.deloitte.com/it/it/pages/life-sciences-and-healthcare/articles/top-10-health-care-innovations.html> accessed 17 December 2020.
[129] 'Re-Open EU' <https://reopen.europa.eu/en/map/LVA/6001> accessed 7 December 2021.
[130] Vayena and others (n 62).
[131] Magdalena Brewczyńska, 'Poland: The Polish Government's Actions to Fight COVID-19: A Critical Look at the "Selfie App" and Direct Access to Location Data' (2020) 6 European Data Protection Law Review 301.

geographical areas. For sovereign states, the declaration of a public health emergency may grant exceptional powers that allow the executive branch to carry out actions without legislative debate[132].

Based on the above premises, the thesis discusses and analyses the example of the Covid-19 pandemic as a health emergency. Considering the philosophical theory on health emergencies, the examples in this thesis on the digital health technologies used in the managing of public healthcare emergencies, consider how privacy and data protection risks associated with the use of such technologies should be ensured.

[132] The state of exception, on the other hand, is often supported by an emergency of some sort, be it a terrorist attack or an earthquake. As observed by Agamben, the state of exception accompanied by the state of emergency permits the state to diminish or supersede constitutional rights[132]. Interestingly, in his work Agamben investigates how a prolonged state of exception deprives individuals of their rights (in his example of dealing with terrorists, the right referred to was citizenship)[132]. It should also be observed that the state of exception is a subjective act, usually the right or power of the sovereign to proclaim such an event[132]. Therefore, the proclamation of the state of emergency can lead to the state of exception and carry with it unwanted consequences. Such consequences may range from temporary suspension of fundamental rights to a long-term removal of such rights such as the right to privacy and data protection.

4 Regulations Surrounding Data Protection, Big Data, and Digital Health Technologies

4.1 Introduction to the Regulatory Landscape

Big data is what powers the digital world. It is the crude oil of the present future: it is unrefined and invaluable. It can be observed that "from the vast and various data collected, value can be retrieved, and that valuable data can be used"[133] in multiple ways. In today's world, multinationals accumulate data and monopolise big data for private purposes, ranging from economic ones and extending to election manipulation, for example, the U.S. elections of 2016, or as we refer to it in this thesis, the private good.

On the other hand, governmental initiatives, coming from places such as the EU, try to facilitate an open data sharing community, focused on the use of big data for the improvement of public services and the public good. For instance, the EU's Data Strategy pays specific attention to the "availability of data for the public good"[134] which is understood in a broad sense and covers areas such as healthcare and environmental protection[135]. Similarly, academic work looks beyond data and requires an establishment of an ethical framework for the "good AI society", also referring to the notion of "common good" and how such "common good" can be enhanced by AI and new technologies[136,137].

Leveraging private and public interests when considering regulation is a continuous challenge. Such a challenge is even more apparent in the context of big data and digital health technologies. It creates an additional hurdle: the nature of big data itself makes it rather impossible to design a legal framework that would address all the risks associated with the collection, processing, storage, use, and reuse of big data. Similarly, it could be argued that the current regulation of digital technologies should be extended to also address the risks which are industry and application specific. For example, risks posed using digital health technologies would differ from risks when using social networks.

In big data in healthcare scenarios, balancing the benefits and risks is even more complicated. In some circumstances, healthcare emergencies can develop into a public healthcare crisis requiring the proclamation of the public healthcare emergency. The adoption of digital health technologies to

[133] Gerybaite and Aurucci (n 54).
[134] European Data Protection Supervisor, 'Opinion 3/2020 in the European Strategy for Data' (2020).
[135] ibid.
[136] Luciano Floridi and others, 'AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations' (2018) 28 Minds and Machines 689 <https://link.springer.com/article/10.1007/s11023-018-9482-5> accessed 2 December 2021.
[137] Bettina Berendt, 'AI for the Common Good?! Pitfalls, Challenges, and Ethics Pen-Testing' (2019) 10 Paladyn, Journal of Behavioral Robotics 44 <https://www.degruyter.com/document/doi/10.1515/pjbr-2019-0004/html> accessed 2 December 2021.

handle such public health crises, is immense. Yet, only some thought has been given as to what risks exist when a state deploys digital technologies for the managing of public healthcare crises. Some authors have examined the fundamental questions of government authority in times of the Covid-19 healthcare crisis, stressing the limits of powers of national governments and sovereigns which are often transnational and data-driven[138].

As already stressed in the previous chapter, big data in healthcare "consists not only of electronic health records, but also includes various structured and unstructured datasets such as clinical decisions, physician's prescriptions, medical imaging, laboratory data, data from biomedical sensors, health-application collected health-related data, and even social network data"[139]. Thus, big data in healthcare may include sensitive, personal records of an individual that should be kept private and confidential, unless explicit consent is given to share such data. In fact, the issue of explicit consent is often mentioned in literature as one of the key data protection issues[140]. While some of such big data may be anonymised or pseudonymised, "the reality is that big data analytic techniques are capable of de-anonymising information using the various analytic tools to re-create a profile of an individual to which the data relates"[141].

The aim of this chapter is three-fold. Firstly, the analysis of the regulatory regime provides a conceptualisation of the complex regulatory background of digital health technologies in the EU and guides as to what extent big data can be used in healthcare without hindering an individual's right to privacy and the right to health. Secondly, through the analysis of the body of law applicable to big data in healthcare, we establish to what extent the use of big data, which includes personal data, is permitted in terms of the data protection legislation in healthcare and what limitations, if any, can be drawn in terms of the processing of such data in emergencies. Thirdly, the thesis identifies and addresses several shortcomings of the existing and proposed regulatory framework at the Union level.

To conceptualise the complex regulatory framework that surrounds big data, digital health technologies, healthcare emergencies, privacy, and data protection this chapter is organised as follows. Firstly, the chapter briefly analyses international and European human rights documents that enshrine the right to privacy, data protection, and the right to health. Among the documents analysed from the human rights perspective, the thesis includes the 1948 Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights Article 17 which

---

[138] Ugo Pagallo, 'Sovereigns, Viruses, and the Law: The Normative Challenges of Pandemic in Today's Information Societies' [2020] SSRN Electronic Journal <https://papers.ssrn.com/abstract=3600038> accessed 21 July 2020.

[139] Gerybaite and Aurucci (n 54).

[140] Alessandro Mantelero, 'Regulating Big data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework' (2017) 33 Computer Law and Security Review 584.

[141] Gerybaite and Aurucci (n 54)

enshrined the protection from interference to one's privacy. In addition, the European Convention on Human Rights is addressed as Article 8 enshrines the right to private life, while the Charter of Fundamental Rights of the European Union protects the right to private and family life in Article 7.
After understanding the human rights framework, the chapter analyses the regulatory framework for big data, privacy, data protection, and digital health technologies in the EU which includes several different legislative instruments. The chapter addresses the several key issues related to the GDPR, which cater for the protection of personal sensitive data, including data concerning health as defined in Article 4(15) of the GDPR. Yet, such processing has its limitations as established in Article 9 of the GDPR. Furthermore, for digital health technologies, the Medical Device Regulation is discussed as it provides an EU-wide framework for the medical devices, their manufacturing, certification, evaluation, and security. As we will find out further on in the work, GDPR becomes a co-requisite for MDR compliance and the issuance of the CE marking for medical devices.
Finally, the chapter considers what role the state of emergency plays in the regulation when it comes to big data, digital health technologies, and the rights to privacy, personal data protection, and health.

4.2 Right to Privacy and the Right to Data Protection in the Context of Human Rights

The regulatory regime surrounding big data in healthcare worldwide can be described as haphazard. Thus, from a methodological point of view, the research chose to limit analysis to the key soft and hard law instruments applicable at the international and European level. We briefly discuss the human rights framework and its influence on the big data regulatory regime within healthcare. In this respect, the chapter starts by considering the historical development of the fundamental rights relevant for the research: the right to personal data protection and the right to privacy. Through the historical development of the two concepts, we establish the importance of the constant protection and the balancing of these rights in the 21st century, considering the technological developments and the introduction of data analytics in the healthcare sector.

4.2.1 On the Protection of the Right to Privacy and the Right to Health at the International Level

The 1948 Universal Declaration of Human Rights (henceforth, the "UDHR") can be considered as one of the founding legislative means to establish fundamental rights to health and privacy. Article 3 of the Declaration provides for the right to life, while Article 25 provides for "the right to a

standard of living adequate for the health and well-being of himself <…> including medical care and <…> the right to security in the event of unemployment, sickness, disability <…>"[142].

Furthermore, Article 12 of the UDHR provides that "no one shall be subject to arbitrary inference with his privacy"[143] establishing a fundamental right to privacy in whatever shape or form expressed. It also includes healthcare as one of the basic pillars.

The development and the recognition of the need to protect the fundamental freedom to privacy were further enshrined in the 1966 International Covenant on Civil and Political Rights. Article 17 of the said covenant introduced protection from "interference with one's privacy, family, home, or correspondence and enshrined the right to protection under the law against such interferences"[144].

4.2.2 On the European Approach to the Right to Health, the Right to Privacy, and the Right to Data Protection

In the European context, the European Convention on Human Rights (henceforth, the "ECHR"), which entered into force in 1953, is considered as the first instrument that gives effects to certain rights enshrined in the UDHR and makes them binding.

Article 8 of the EU Convention on Human rights enshrines the "right to private and family life"[145]. Interestingly, Article 15 of the same convention provides for the possibility of derogations in times of emergencies, such as public health emergencies, indicating that privacy is not an absolute right[146]. It should be noted that the development and the expansion of the early EU did not consider fundamental freedoms in its treaties. However, this changed with the adoption of the Charter of Fundamental Rights of the EU in the year 2000 and its entry into force in 2009, obtaining the same legal value (status) as the treaties of the European Union.

The EU CFR articles not only encompass the right to private life enshrined in Article 7, but also specifically protect personal data, in Article 8, through the laying down of the principles for data processing: fairness, purpose, consent, legitimate basis, right of access, right of rectification. These principles also form the basis of the principles enshrined in the primary data protection legislation in the EU, the GDPR. Lastly, the EU CFR also enshrines the right to health care in Article 35, establishing that "everyone has the right of access to preventive health care and the right to benefit

[142] 'Universal Declaration of Human Rights | United Nations' <https://www.un.org/en/universal-declaration-human-rights/> accessed 17 January 2020.
[143] ibid.
[144] OHCHR | International Covenant on Civil and Political Rights.
[145] 'European Convention on Human Rights' <https://www.coe.int/en/web/human-rights-convention> accessed 18 March 2020.
[146] European Court of Human Rights, 'Guide on Article 15 of the European Convention on Human Rights Derogation in Time of Emergency'.

from medical treatment under the conditions established by national laws and practices"[147]. Throughout its existence, the ECtHR played a crucial role in ensuring the protection of fundamental human rights. Further sections of this chapter will illustrate how the ECtHR ensured the protection of the fundamental rights to health, privacy, and data protection.

4.2.3 On the Evolution of the Right to Privacy and the Right to Health

This historical perspective into the right to health and the right to privacy indicates two things. One, that the right to private life and privacy have been acknowledged as fundamental rights that survive changing times. Second, that there has been a fundamental shift from the right to privacy and private life to the right of data protection. This fundamental shift is connected solely to the development of digital technologies such as computers and data analytic tools in the past decades. The 1973 report published by Willis H. Ware titled "Records, Computers, and the Rights of Citizens" addressed the risks of the use of personal data systems that laid foundations on which the data protection law in the EU, the GDPR, has been built upon[148].

Consequently, the dawn of the digital age brought about the shift from the right to privacy to the right of data protection and facilitated the development towards the protection of personal data by expanding the scope of the rights connected to individual personality rights which may be threatened by the collection or processing of personal data.

4.3 Critical Analysis of Selected Data Protection Related Issues in the Context of Big Data and Digital Health Technologies

In Europe, the digital health technology regulatory field is heavily fragmented and highly dependent on health technology developed, its function, and the targeted audience[149,150]. The evolving nature of such devices from IoT towards IoE, which may be described as an interconnected relationship between devices, people, processes, and data, make it even more complicated to regulate this field. This interconnected relationship between these actors and processes entail a level of relationship between digital health technologies, big data, data protection, and cybersecurity.

---

[147] 'EU Charter of Fundamental Rights | European Commission' <https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en> accessed 18 March 2020.

[148] Willis H. Ware, *Records, Computers, and the Rights of Citizens: Report*, vol 10 (Department of Health and Education of the United States of America ed, 1973).

[149] Bart van der Sloot and Sascha van Schendel, 'Ten Questions for Future Regulation of Big data: A Comparative and Empirical Legal Study' (2016) 7 Journal of Intellectual Property, Information Technology and Electronic Commerce Law <https://heinonline.org/HOL/Page?handle=hein.journals/jipitec7&id=116&div=16&collection=journals> accessed 4 November 2019.

[150] Alessandro Mantelero and Giuseppe Vaciago, 'Data Protection in a Big data Society. Ideas for a Future Regulation' (2015) 15 Digital Investigation 104.

In research, substantial attention has been dedicated to studying data protection challenges associated with big data. It has been argued that the GDPR may be able to tackle the legal challenges of big data[151]. Some authors have also indicated that "<…> the new Regulation[152] is mainly aimed at companies handling large amounts of data"[153].

Furthermore, as noted by Pagallo, in data protection, the role of consent has been the primary focus of the research[154]. Nonetheless, it can also be argued that in big data and digital health context research focuses on the importance of the Data Processing Impact Assessment (henceforth, the "DPIA"), and the notions of personal data and data concerning health. Today, some digital health technologies such as fitness or diet applications may only require compliance with the GDPR.

Nonetheless, other digital health technologies, such as smartwatches with ECG software, may require a more specific regulatory compliance not only in terms of data protection, but also in terms of device safety and security which falls under the MDR scope. To add a layer of complexity, digital health technologies have a requirement to comply with the cybersecurity standards which are particularly relevant for digital health technologies. To complicate the matter even further, digital health technologies used to manage healthcare emergencies may require compliance with additional ad-hoc regulatory requirements.

Therefore, the section provides a critical analysis of the selected GDPR=related issues in the context of big data and digital health technologies.

4.3.1 The Importance of Personal Data in Big Data and Digital Health Technology Context

The entry into force of the European General Data Protection Regulation on 25th May 2018 is the crown jewel of the EU data protection authorities symbolising the new era of personal data protection for the individual. It exponentially increased individuals' rights over how their personal data is collected, processed, or stored. Amongst other things, the GDPR has also introduced the "right to be forgotten", a unique right for the EU citizen's personal data to be deleted upon request and under certain circumstances.

In the context of big data, one can observe that personal data protection becomes a greater issue. In this respect, the purpose limitation principle enshrined in the GDPR requires that "personal data

[151] Ugo Pagallo, 'The Legal Challenges of Big data: Putting Secondary Rules First in the Field of EU Data Protection' (2017) 3 European Data Protection Law Review (EDPL) 34 <https://iris.unito.it/handle/2318/1640445> accessed 12 November 2019.

[152] Authors note: the GDPR

[153] Pompeu Casanovas and others, 'Regulation of Big data: Perspectives on Strategy, Policy, Law and Privacy' (2017) 7 Health and Technology 2017 7:4 335 <https://link.springer.com/article/10.1007/s12553-017-0190-6> accessed 2 December 2021.

[154] Pagallo, 'The Legal Challenges of Big data: Putting Secondary Rules First in the Field of EU Data Protection' (n 151).

must be collected for specified, explicit, and legitimate purposes"[155]. Such limitation may be impossible to achieve is some of big data scenarios where the purpose of the collection is unclear at the time of collection[156]. While concerns such as the purpose limitation principle have been discussed extensively in the state-of-the-art, only some research has been conducted on the notion of personal data as the underlying requirement for the protection of the GDPR, and the extension of the same to big data context.

In this regard, the drafters of the GDPR decided to divide data into two distinct categories: personal and non-personal data. Such distinction, after all, was necessary for the scope of the regulation as it should have been clear what type of data is protected under the new (at the time) regulatory regime. Such approach is still criticised by both industry experts and the academia as not considering technological developments of big data analytics tools which blur the line between personal data and big data, making big data incompatible with the GDPR[157,158].

This thesis tends to disagree with such incompatibility. While the notion big data is not explicitly defined in the text of the GDPR, nonetheless, the interaction between big data and data protection is rather profound. To start with, Article 4 of GDPR introduces the notion of personal data. The language of GDPR indicates that the term personal data:

"Means 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 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"[159].

Already, the said article gives a rather vague description of personal data, providing the reader with a wide range of generic examples for interpretation of what could be considered personal data.

Nonetheless, the importance of the distinction between what should be considered personal data and what should not in the context of big data is more complicated. Drawing a sharp line between the

[155] Article 29 Data Protection Working Party (n 44).

[156] Nikolaus Forgó, Stefanie Hänold and Benjamin Schütze, 'The Principle of Purpose Limitation and Big data' [2017] Perspectives in Law, Business and Innovation 17 <https://link.springer.com/chapter/10.1007/978-981-10-5038-1_2> accessed 10 December 2021.

[157] Tal Z Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2016) 47 Seton Hall Law Review <https://heinonline.org/HOL/Page?handle=hein.journals/shlr47&id=1019&div=37&collection=journals> accessed 3 June 2020.

[158] Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Overstretched Scope of EU Data Protection Law' [2017] SSRN Electronic Journal.

[159] The European Parliament and The Council Regulation (EU) 2016/679 of the European Parliament and 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 (n 9).

two concepts on the types of data may be considered as a simplification of the attempts to transpose an individual's personality, at least in part, into the digital world. This blurred line between personal data, non-personal data, and big data often creates a "network effect" where, due to big data analytics, personal data protection effects may spill over onto others, for example, because of the same piece of data relating to a group of people, such as genetic data[160]. Thus, one would fall short if they argued that personal data refer only to such definable features as birth date, name, or surname. Similarly, one could find it also hard to fully support the argument that personal data is also data that refers to indefinable features such as "one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of a natural person"[161] as defined in Article 4(1) of the GDPR.

Data is context-driven. As the above-mentioned example illustrates, the same data in one context may be considered personal, while in another it may not. For instance, anonymised social network data would not be considered personal, however, if it were combined with another data source, such data could become personal due to inferences that could be made with data analytics.

This leads us to another argument. As observed by Fink, "from a technical perspective the increasing availability of data points, the continuing sophistication of data analysis algorithms, and performant hardware"[162] make it simpler "to link datasets and infer personal information from ostensibly non-personal data"[163]. Even further, some scholars argue that "the legal test to differentiate between personal and non-personal data is embodied in Recital 26 GDPR"[164] which refers to the act of pseudonymisation of personal data attributable to a specific individual. Other scholars argue that the use of the terms such as personal data in the GDPR is incompatible with the big data age as the GDPR is not capable of addressing the risks that come with the technological advancements and the free flow and open data initiatives[165].

It can be observed that the term big data does not feature in the text of the GDPR, not because the legislators did not account for big data, but because of the legislator's focus on the personal category of data within the context of big data itself. However, this approach may also be criticised. It could be argued that the GDPR creates an illusion of protection of personal data through the

---

[160] Sylvie Delacroix and Neil D Lawrence, 'Do Property Rights in Personal Data Make Sense after the Big data Turn?: Individual Control and Transparency' (2017) 9 International Data Privacy Law 236 <https://papers.ssrn.com/abstract=3070228> accessed 10 December 2021.

[161] The European Parliament and The Council Regulation (EU) 2016/679 of the European Parliament and 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 (n 9).

[162] Michèle Finck and Frank Pallas, 'They Who Must Not Be Identified - Distinguishing Personal from Non-Personal Data Under the GDPR' [2019] SSRN Electronic Journal <https://papers.ssrn.com/abstract=3462948> accessed 2 December 2021.

[163] ibid.

[164] ibid.

[165] Zarsky (n 158).

proclamation of various rights that individuals are entitled to. This illusion, however, vanishes due to the lack of vigorous enforcement mechanisms of GDPR in both private and public sectors. This is especially evident in cases of major cross-border complaints where big-tech players have the resources to handle such data while public authorities do not[166].

Finally, Article 4(15) of GDPR includes the term data concerning health[167] which is described as "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"[168], which is independently examined in the subsequent paragraph.

4.3.2 The importance of Data Concerning Health and Article 9 in Big Data and Digital Health Technology Context

As mentioned above, one particularity of big data in the context of GDPR and within privacy is that big data is highly context dependent. Big data sets may include personal data, which would supposedly make the big dataset itself subject to the GDPR. However, big data sets do not necessarily contain personal information in the strict sense of personal data referred to under the GDPR, yet dependent on the context, the same big data set may be data of a personal nature or become personal if it can be attributed to a specific individual.

Hence, big data could become subject to the GDPR due to big data analytic tools used for analysing such data. For instance, in 2006 Arvind Narayanan and Vitaly Shmatikov, from the University of Texas at Austin, published a research paper in which they deployed a de-anonymisation methodology on Netflix's Prize Data set[169]. The said data set included personal anonymised data and through big data analytics, the researchers were able to re-identify and link data to a particular individual using IMDB as a source for background knowledge. Using a de-anonymisation methodology, the research was able to link the micro-data in Netflix's dataset not only to an individual, but also uncover the individual's personal sensitive data including political preferences, religious views, and potential sexual orientation.

The above example came out pre-GDPR; nevertheless, it illustrates well the potential risks of big data analytics tools to personal data protection, not only in this scenario but also in the context of digital health as well. A similar example could also be imagined in the digital health scenario. For instance, a healthcare entity that stores anonymised electronic patient records and health-related

[166] Lydia Lundstedt, 'International Jurisdiction over Crossborder Private Enforcement Actions under the GDPR' [2018] SSRN Electronic Journal <https://papers.ssrn.com/abstract=3159854> accessed 2 December 2021.

[167] The European Parliament and The Council Regulation (EU) 2016/679 of the European Parliament and 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 (n 9).

[168] ibid.

[169] Arvind Narayanan and Vitaly Shmatikov, 'Robust De-Anonymization of Large Sparse Datasets'.

data from various patient digital health devices (such as, ECG monitors, sleep monitoring devices and so on). The more data points a healthcare entity obtains, the more sophisticated its data analytics algorithms are, the easier it would link these different data points to a particular individual, thus making such data potentially belonging to a special category of data included in Article 9 of the GDPR.

Data concerning health is defined in Article 4(15) of the GDPR as 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"[170]. In this respect, data concerning health is considered a separate category of personal data under Article 9 of GDPR and requires an additional level of protection. In practical terms, this means that anyone using data that may be considered as data concerning health must adhere to stricter legal requirements for the processing of such data.

Article 9(1) of the GDPR prohibits the processing of special categories of data unless such processing is done under one or more of the exemptions established in Article 9(2) of the GDPR. The said article provides a list of exemptions for the processing of data concerning health which include:

1. "explicit consent to the processing (Article 9(2)(a));
2. processing is necessary for carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law (Article 9(2)(b));
3. processing 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 (Article 9(2)(c));
4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body (Article 9(2)(d));
5. processing relates to personal data which are manifestly made public by the data subject (Article 9(2)(e);
6. processing is necessary for the establishment, exercise, or defence of legal claims or whenever courts are acting in their judicial capacity (Article 9(2)(f));
7. processing necessary for the reasons of substantial public interest (Article 9(2)(g));
8. processing necessary or reasons of preventative or occupational medicine (Article 9(2)(h));
9. processing necessary for reasons of public interest in the area of public health (Article 9(2)(i));

[170] The European Parliament and The Council Regulation (EU) 2016/679 of the European Parliament and 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 (n 9).

10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes under Article 89(1) (Article 9(2)(j))"[171].

The derogations that are discussed in this thesis are: Article9(2)(a); Article 9(2)(c); Article 9(2)(g); Article 9(2)(h); and Article 9(2)(i) of the GDPR.

Article 9(2)(a) provides an exemption for the processing of sensitive personal data where a data subject has given explicit consent for such processing under the said article. In comparison to Article 6(1)(a) of the GDPR which simply requires the consent of a data subject for the processing of personal data, Article 9(2)(1) provides a higher threshold for the processing of sensitive data. In this regard we should note that explicit consent means that consent cannot be implied, thus requiring a higher degree of meticulousness, definiteness, and accurate description of the purpose of processing when a declaration of consent is drafted and provided for a data subjects' signature[172]. In addition, controllers under the GDPR must provide data subjects with clear information about the option to withdraw consent at any time when consent, including explicit consent, is used as the basis for processing.

Also, Article 9(2)(c) covers the exemption for processing of sensitive data when such processing could protect "the vital interests of the data subject or another natural person where the data subject is physically or legally incapable of giving consent"[173]. Recitals 46 and 112 of the GDPR provide a brief explanation of such processing. For instance, Recital 46 states that the exemption to the processing of sensitive data under Article 9(2)(c) should cover instances such as the protection of "an interest which is essential for the life of the data subject or that of another natural person"[174]. Recital 112 further elaborates that processing "should be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests"[175]. Such vital interests include "physical integrity or life if the data subject is incapable of giving consent"[176]. To put this in the context of digital healthcare, take an example of sensitive data needed for medical treatment of a car crash patient. To process sensitive data under this exemption, the controller would be required to assess several conditions. First, the controller would have to establish that the person (data subject) is not capable him/herself to give consent. For instance, because they are legally incapable of giving consent in cases such as being under duress, being a minor, or being officially declared as incapacitated subject, or because the data subject cannot

[171] ibid.
[172] Mantelero (n 141).
[173] The European Parliament and The Council Regulation (EU) 2016/679 of the European Parliament and 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 (n 9).
[174] ibid.
[175] ibid.
[176] ibid.

physically give consent due to serious illness, for example being in a coma. Second, the controller would have to address the data protection interests of a data subject at hand and their vulnerability to the processing of sensitive data, as well as the vulnerability and exposure of other natural persons to the processing of such data, i.e., balancing test whether the processing of sensitive data would lead to benefits for the data subject and any other natural person.

Article 9(2)(g) of GDPR covers an exemption for the processing of sensitive data to protect substantial public interest. This exemption for the processing of sensitive data takes on another dimension as it is aimed at protecting the public at large and thus intrinsically it is likely that the processing of sensitive data would be done on a large scale. The said exemption establishes several conditions to be addressed before the processing takes place.

First, the controller must establish that the processing of sensitive data is proportionate to the aim pursued. Second, the controller must establish that the 'essence of the right to data protection' is respected. Third, the controller must establish suitable and specific measures to safeguard the fundamental rights and interests of a data subject.

Yet, the real concern with this exemption is what is meant by substantial public interest. It can be observed that the lack of precise formulation of substantial public interest may refer to a public interest but also a specific public interest, such as public healthcare, which is addressed by a separate paragraph of the said article[177,178]. Additionally, Recital 46 provides little guidance and mentions examples of data processing that serves important grounds of public interest such as humanitarian purposes, including monitoring of epidemics, or man-made disasters.

In addition, Article 9(2)(h) covers a broad exemption for the processing of sensitive data for healthcare and the provision of health purposes. Processing activities that are covered, inter alia, include preventative or occupational medicine, medical diagnosis, provision of social care or treatment and so on. Yet, the said provision does not include an exemption for health research which is covered under Articles 9(2)(i) and 9(2)(j). The said article, however, includes safeguards for such processing that are further referred to in Article 9(3), which provides that sensitive data must be processed by or under the supervision of a professional such as a doctor, hospital, and under applicable professional secrecy provisions as determined under the Union or Member State law.

Finally, Article 9(2)(i) of the GDPR encompasses an exemption for the processing of sensitive data for public interest in public health. Under the said article public health is to be understood in a

[177] David A. Frenkel* and David M. Wood, 'PATIENTS' RIGHT TO PRIVACY AND PUBLIC INTEREST' (2015) 34 Medicine and Law 85.

[178] John MM Rumbold and Barbara K Pierscionek, 'A Critique of the Regulation of Data Science in Healthcare Research in the European Union' (2017) 18 BMC Medical Ethics 27 <http://bmcmedethics.biomedcentral.com/articles/10.1186/s12910-017-0184-y> accessed 4 December 2019.

broad manner as stated in Recital 54 which refers to the notion of public health contained in Regulation 1388/2008. Yet, Article 9(2)(i) specifies that this exception applies particularly in cases such as when processing is required for protecting against serious-cross border threats to health or ensuring quality and safety of healthcare or medicinal products[179]. As with other exemptions, conditions must be satisfied for the processing of sensitive data under Article 9(2)(i). First, processing activity must be considered to protect the public interest in public health. Second, processing must be allowed "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"[180]. Third, the controller must ensure that such data is not processed for other purposes or by third parties. Lastly, the right to be forgotten contained in Article 17 of the GDPR does not apply to data processed under this exemption (art. 17(3) GDPR).

4.3.3 The Significance of the Data Protection Impact Assessment for Digital Health Technologies and Big Data

The GDPR undeniably plays a significant role in the development of digital health technologies that use big data. The GDPR may be the instrument that limits the use of health-related data for the development of new technologies or ensure the protection of health-related data which is processed throughout various digital health technologies.

In this respect, Article 35 of the GDPR incorporates a requirement for a DPIA to be carried out in cases where the 'use of new technologies' results "in a high risk to the rights or freedoms of natural person"[181]. Article 35 of the GDPR enshrines that:

"Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks"[182].

---

[179] The European Parliament and The Council Regulation (EU) 2016/679 of the European Parliament and 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 (n 9).

[180] ibid.

[181] Shakila Bu-Pasha, 'The Controller's Role in Determining "High Risk" and Data Protection Impact Assessment (DPIA) in Developing Digital Smart City' [2020] https://doi.org/10.1080/13600834.2020.1790092 391 <https://www.tandfonline.com/doi/abs/10.1080/13600834.2020.1790092> accessed 29 July 2022.

[182] The European Parliament and The Council Regulation (EU) 2016/679 of the European Parliament and 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 (n 9).

We may argue that GDPR's Article 35 addresses and is also applied to big data scenarios. In fact, we can observe from the wording of Article 35 of the GDPR and its requirements for a DPIA to be carried in situations where data that would be processed using new technologies. In addition, as specifically mentioned in Article 35 of GDPR, such processing must consider the scope of the processing, i.e., the volume of data and the envisaged impact it would have on the protection of personal data.

Moreover, Article 35 envisages that the "supervisory authorities of the Member States may also establish and make public a list of the kind of processing operations"[183] that would require a DPIA. Such a list includes, inter alia, processing activities of sensitive data, which also includes data concerning health. It could be argued that the best practice in processing data concerning health is to carry out a DPIA before any processing activity takes place.

Furthermore, it should be noted that the GDPR does not define large-scale data and little guidance is provided on this in Recital 91 of the GDPR, which specifically indicates large-scale processing operations. Such operations often are set to process a large amount of personal data at national, or even supranational level. Also, such processing "could affect many data subjects and likely result in high-risk processing"[184]. Likewise, in cases where "new technology is used on a large scale to process operations which result in a high risk to the rights and freedoms of data subjects, where those operations render it more difficult for data subjects to exercise their rights"[185], the WP29 provides recommendations onwhat would constitute large-scale processing of data. The WP29 guidelines include the following criteria:

"a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
b. the volume of data and/or the range of different data items being processed;
c. the duration, or permanence, of the data processing activity;
d. the geographical extent of the processing activity"[186].

[183] 'Data Protection | European Commission' <https://ec.europa.eu/info/law/law-topic/data-protection_en> accessed 28 July 2022.
[184] Art. 29 WP, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (2017) WP 248 rev Article 29 Working Party 22.
[185] 'Data Protection | European Commission' (n 184).
[186] Art. 29 WP (n 185).

The guidance provided by the WP29 directly refers to the 3Vs of big data: volume, velocity, and variety, indirectly including big data processing in the scope of GDPR only to such an extent it creates risks to the protection of personal data.

To support the Member States in assessing when processing would require a DPIA, in 2017 the Working Party 29 published Guidelines on DPIA and determining whether the processing is "likely to result in a high risk" for the purposes of the GDPR. The above-mentioned WP29 guidelines established a list of nine processing activities which would provide the supervisory authorities of the Member States with a list of activities that are "likely to result in a high risk"[187] to the protection of personal data and thus would require a DPIA. The processing activities include:

1. "Evaluation or scoring;
2. Automated decision making with legal or similar significant effect;
3. Systematic monitoring;
4. Processing of sensitive data or data of a highly personal nature;
5. Data processed on a large scale;
6. Matching or combining datasets;
7. Data concerning vulnerable data subjects;
8. Innovative use or applying new technological or organisational solutions;
9. When the processing in itself "prevents data subjects from exercising a right or using a service or a contract"[188].

To compare how Member States have transposed the above-mentioned guidelines, this research has sampled and analysed five lists provided by the Member States on the EDPB's website against the Working Party's 29 Guidelines on DPIA on determining whether the processing is "likely to result in a high risk" for GDPR, adopted in 2017. The results of the analyses are summarised in Table 3, below.

[187] ibid.

[188] Working Party 29, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679, ' (2017) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236> accessed 9 June 2020.

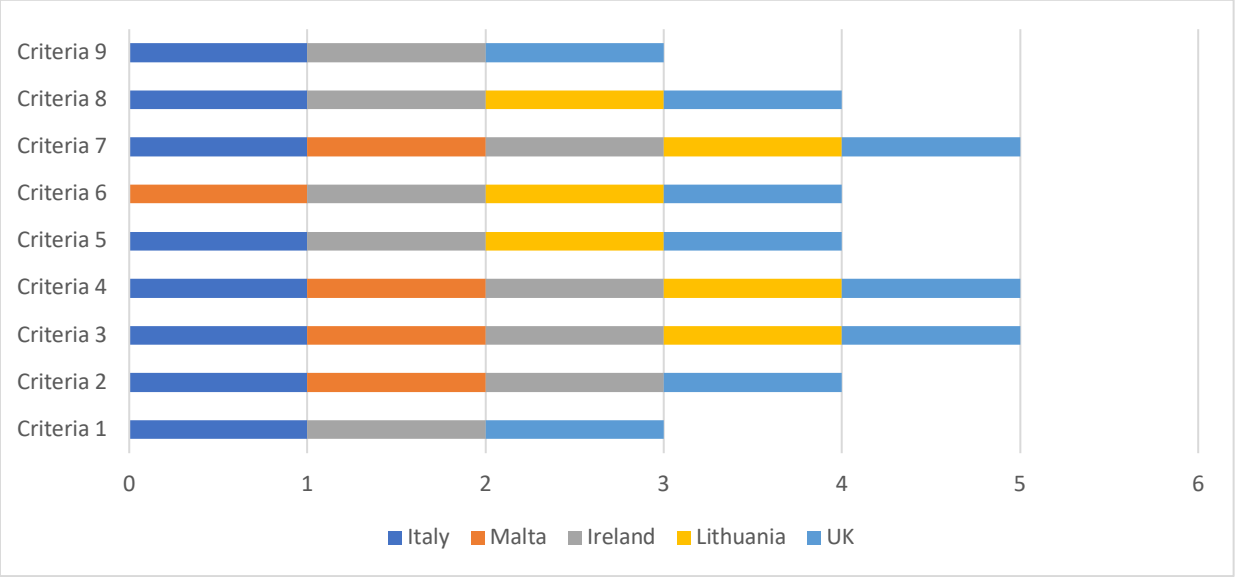

Table 3. Results of the analysis on processing which is "likely to result in a high risk"

Several observations can be made from the above analysis. First, the Member States' transposition differs greatly due to the tool (guidelines) used for said transposition. Guidelines do not require mandatory transposition and thus leave it to the Member States' discretion to decide which parts to adopt and which not. Such liberty also leads to the conclusion that there is a lack of a common European understanding and approach not only to DPIA but also to big data.

Second, it can be observed that only three out of nine processing activities were identified by all the Member States as processing activities that are "likely to result in a high risk" for the protection of personal data. Such activities include systematic monitoring (criteria 3), processing of "sensitive data or data of a highly personal nature"[189] (criteria 4), and "data concerning vulnerable data subjects"[190] (criteria 7). Third, only two of the analysed Member States transposed the provided criteria in full, Ireland and the UK, with Italy requiring a DPIA to be carried for eight processing activities, while smaller Member States such as Malta have included the requirement for DPIA only for five out of the nine indicated activities. Lastly, the WP29 guidelines specifically indicate that a DPIA should be carried out in cases of data processed on a large scale (Criteria 5). This suggests that even though the articles of GDPR do not directly name big data in its text, the GDPR still considers the risk and impact big data may have on the protection of personal data. Similar can be confirmed from the analyses as four out of five Member States transposed such criteria into their national legislation.

[189] Art. 29 WP (n 185).
[190] ibid.

4.4 Ensuring Data Protection in Digital Health Technologies Through the Medical Devices Regulations Regulatory Framework

While the GDPR addresses the protection of data concerning health, the regulatory landscape surrounding big data, data protection, privacy, and digital health technologies expands beyond the GDPR. In this respect, we further analyse how the 2017 EU Medical Devices Regulation[191] safeguards the fundamental rights to data protection and privacy through safety and security of medical devices entering the EU market. In this respect, some authors have already addressed how secondary mechanisms of legal coordination in regulation can prevent threats and risks of fragmentation due to complex interaction between several converging EU regulations[192]. Hence, this part of the chapter provides a critical analysis of the MDR regulatory regime considering big data, digital health technologies, and data protection. Specifically, the following subchapters of the thesis present that the MDR, as a harmonised regulation, sets up mechanisms of legal coordination, cooperation, and legal co-requisite approach to prevent the fragmentation of the legal system in the complex digital health technology environment.

4.4.1 MDR at the Core of Digital Health Technology Regulatory Regime in the EU

IoE may be described as an interconnected relationship between devices, people, processes, and data[193,194]. This interconnected relationship entails a level of relationship between digital health technologies, data protection and cybersecurity. In Europe, the digital health technology regulatory field is heavily fragmented and highly dependent on the health technology developed, its function and targeted audience. In this respect, digital health technologies encompass a variety of technologies, such as mHealth devices and applications, medical devices, and health-related technologies. Some consumer mHealth devices such as fitness applications may only require compliance with the GDPR, while other mHealth devices such as smartwatches may require a more specific regulatory compliance, not only in terms of data protection but also in terms of device

[191] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EE

[192] Pagallo, 'The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection' (n 151).

[193] Dave Evans, 'The Internet of Everything How More Relevant and Valuable Connections Will Change the World' (2015).

[194] Shuo Tian and others, 'Smart Healthcare: Making Medical Care More Intelligent | Elsevier Enhanced Reader' (2019) 3 Global Health Journal <https://reader.elsevier.com/reader/sd/pii/S2414644719300508?token=2DFD351672D716CA6F7C0238A312A612A67C19A26EC8489A30588D1A0263CD4B783ECB07BEDDB375A9EE63EA4C792FDA&originRegion=eu-west-1&originCreation=20210520112219> accessed 20 May 2021.

safety and security[195]. Perhaps the most well-established regulatory regime for digital health technologies in Europe is the EU's MDRs. The MDR's predecessor, the Medical Device Directive ("MDD") has been highly criticised due to its systemic focus to protect commercial interests and innovation above the health of its citizens[196]. Also, to date, the MDD has been criticised for the failure to harmonise medical device safety and ensure their security due to inadequate standards for such devices[197].

MDR is a complex piece of legislation that lays down rules concerning the entry into the European market of safe and secure medical devices. The regulatory regime covers non-in vitro medical devices while regulation 2017/46 covers in vitro diagnostic medical devices ("IVDR"). These two regulations aim to ensure that only high quality, safe and secure digital medical devices circulate in the internal market, with the ultimate objective being to protect the patients of such devices.

The MDR takes on the challenge to rectify the MDD's shortcomings. "Positive integration" is the chosen way to deal with such shortcomings[198]. In this respect, the MDR establishes common rules and standards throughout the EU for medical devices. These common rules and standards allow medical devices to ensure their conformity with EU regulations which is assured by Notified Bodies (henceforth, the "NB"). The NBs are private assurance entities that carry out the regulatory compliance assessment of the medical devices entering the EU market. Once the NB assesses the medical device's compliance with the MDR, the medical device can be given a European conformity "CE" label, allowing the medical device to circulate freely in the EU.

4.4.2 The Evolving Nature of Medical Devices

With this background in mind, we ought to explore the interconnectivity of health IoE and EU MDR's definition of medical devices. Article 2(1) of the MDR encompasses a broad definition of what may constitute a medical device which includes, inter alia, any instrument, apparatus, software, or appliance for human beings which can be used alone or in combination, for one or more specific medical purposes[199,200,201]. Such medical purposes may include diagnosis, prevention

---

[195] The most prominent example is Apple watches that in certain EU jurisdictions fall under the MDR regulatory regime (specifically, the ECG software is considered a medical device)

[196] Holly Jarman, Sarah Rozenblum and Tiffany J Huang, 'Neither Protective nor Harmonised: The Crossborder Regulation of Medical Devices in the EU' [2020] Health Economics, Policy and Law 51.

[197] ibid.

[198] ibid.

[199] Paul Quinn, 'The EU Commission's Risky Choice for a Non-Risk Based Strategy on Assessment of Medical Devices' (2017) 33 Computer Law and Security Review 361 <http://dx.doi.org/10.1016/j.clsr.2017.03.0190267-3649/www.sciencedirect.com> accessed 26 May 2021.

[200] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EE.

[201] MDR, Article 2(1): "'medical device' means any instrument, apparatus, appliance, software, implant, reagent,

or prognosis of diseases, disability injury, an inexhaustive list which is to be determined on a case-by-case basis[202,203].

The broad definition of the medical device under the MDR is the starting point connecting the health IoE with the regulatory world[204]. In fact, with this seemingly all-encompassing definition of medical device, the MDR seeks to underline a natural evolution of various mHealth, telehealth and eHealth consumer applications and similar devices[205] into legitimate medical devices. Some of our well-being devices such as the Apple Watch have some of their software and wearables compliant with the MDR and carry with them the CE mark. Similarly, software, in its own right, or when used in combination with another device may be considered as a medical device and would require regulatory compliance.

The MDR and its recitals[206] attempt to treat various digital health technologies, such as consumer health applications, devices, and software strictly: as either a medical device or not. Yet, there is no clear distinction between the interpretation of what is considered a medical device and what is not. Moreover, the use of terms such as lifestyle and well-being raise doubts as to what would be considered a medical device under the regulation. For instance, if lifestyle and well-being devices, applications or software have a direct impact on an individual's health, could this not be considered as a broad, all-encompassing purpose to keep an individual healthy, thus having a medical purpose of prevention of illness? So far, few clarifications have been provided in this respect. The lack of clarity in this respect has been also demonstrated by a study of the German application store for

---

material or other Article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:
— diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,
— diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,
— investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,
— providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations,
and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means. The following products shall also be deemed to be medical devices:
— devices for the control or support of conception;
— products specifically intended for the cleaning, disinfection or sterilisation of devices as referred to in
Article 1(4) and of those referred to in the first paragraph of this point." ibid.

[202] Quinn (n 200).

[203] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EE.

[204] Adrian Thorogood and others, 'Genetic Database Software as Medical Devices' (2018) 39 Human Mutation 1702.

[205] Otherwise known as "well-being devices".

[206] MDR Recital 19: "[...] Software in its own right, when specifically intended by the manufacturer to be used for one or more of the medical purposes set out in the definition of a medical device, qualifies as a medical device, while software for general purposes, even when used in a healthcare setting, or software intended for life-style and well-being purposes is not a medical device". Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/ 2017.

health apps, which tested the conformity of such health apps against the regulatory requirements under the MDR for the CE marking[207]. The findings of the study were eye-opening, as the CE marking "seems to be irrelevant for manufacturers"[208].

4.4.3 Qualification as a Medical Device Versus Classification of a Medical Device

It is often thought that the qualification of consumer digital health technologies as medical devices under the MDR depends on the harm they may pose or on their function. Yet, the qualification of a digital health technology, be it a consumer application, software, or a device, highly depends on the intended purpose of the device. Therefore, to ultimately qualify as a medical device, a digital health technology must be "intended to be used, alone or in combination, for one of the medical purposes"[209] that are listed in Article 2(1) of the MDR. Such intended purpose is decided by the manufacturer through appropriate labelling, instructions for use, and any marketing and sales materials (MDR art. 2(12)). A safeguard from misleading the end-user and patient as to the intended purpose is provided in Article 7 of the MDR. The safeguard is mostly focused on promotional and marketing materials. For instance, for apps, the application store description, the category in which it is offered for sale, the advertisements, the landing page, and the developer's social media channels would be relevant.

Even if a digital health technology, such as a health application or software, do not fall within the definition of a medical device, manufacturers and developers still ought to assess if these could be considered an "accessory" to a medical device[210]. It should be noted that (digital) accessories may also fall under the MDR framework and carry their regulatory requirements.

On another note, classification of a digital health technology as a medical device is done once the device is qualified as a medical device under the MDR. The classification of the device is based on the harm it may pose to the patient. In essence, the classification rules contained in Annex VIII establish the appropriate conformity assessment procedure: the higher the classification of a medical device, the greater the level of assessment required from the Notified Body[211]. The higher the classification of a medical device, the more stringent the applicable regulatory compliance requirements for a particular medical device are i.e., the higher risk of harm to the patient, the

---

[207] Urs Vito Albrecht, Uta Hillebrand and Ute von Jan, 'Relevance of Trust Marks and CE Labels in German-Language Store Descriptions of Health Apps: Analysis' (2018) 6 JMIR mHealth and uHealth </pmc/articles/PMC5943626/> accessed 9 June 2021.

[208] ibid.

[209] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/.

[210] Minssen, Mimler and Mak (n 81).

[211] Magali Contardi, 'Changes in the Medical Device's Regulatory Framework and Its Impact on the Medical Device's Industry: From the Medical Device Directives to the Medical Device Regulations' (2019) 12 Erasmus Law Review 166.

higher the classification and thus the regulatory requirements in terms of medical safety and security are applicable. These safety and security requirements, for the purposes of the MDR, may require surpassing certain data protection standards. For example, access to patient data at the hospital is usually limited to the necessary personnel. In the case of a medical device which deals with high-risk health problems (e.g., vital signs), the purpose of the medical device may require the developers to expand access to data to, e.g., emergency room personnel, in cases where there is imminent threat or risk to patient's life.

4.4.4 The Blurred Line Between Digital Health Technologies and Medical Devices: The Case of Intended Purpose

As mentioned above, the intended purpose of the manufacturer of the medical device takes a primary role in establishing whether a device qualifies as a medical device. Besides the fact that the intended purpose is, first and foremost, the responsibility of the device manufacturer, the MDR also provides a questionable oversight mechanism on the qualification of a device. While the intended purpose is the responsibility of the manufacturer, some authors suggest that the intended purpose should be formulated by a medical, regulatory, or quality professional and for the intended user group in the appropriate medical language[212].

The qualification of the device is further assessed by the NB in the technologies or devices' compliance evaluation. The NB is selected by the manufacturer of the potential medical device. This may be considered the first red flag of the MDR. The interdependent relationship between the manufacturer of a potential medical device with an NB is a typical B2C relationship. It raises questions whether an NB can be truly impartial when assessing compliance with the MDR of its client's device, after all, a positive assessment outcome could directly impact NB's financial success. Such an approach also encourages forum-shopping whereas a manufacturer may search for an NB with lax standards for compliance[213]. This European approach is highly criticised and vastly differs from the U.S. approach where a centralised authority (namely the Food and Drugs Administration or FDA) assesses the conformity of medical devices[214].

The second red flag of the MDR is that the regulation is vague as to what is to be considered as the intended purpose and does not specify the degree of the intended purpose of the potential medical device. Such lack of specificity calls for the need to establish degrees or other abstractions of

[212] Quinn (n 200).

[213] 'Statement from Jeff Shuren, M.D., J.D., Director of the Center for Devices and Radiological Health, on Updated Safety Communication about Rates of Duodenoscope Contamination from Preliminary Postmarket Data | FDA' <https://www.fda.gov/news-events/press-announcements/statement-jeff-shuren-md-jd-director-center-devices-and-radiological-health-updated-safety> accessed 26 May 2021.

[214] Jarman, Rozenblum and Huang (n 197).

intended purpose due to the specific nature, design, and attributes of certain categories of medical devices, such as software. Unlike medical equipment, which could be considered as a stringboard case of a medical device, the design and use of digital health technologies, such as medical software or apps, may be deceptive. For example, the explicit intended purpose as marketed by the developer of a software or an application may contradict the implicit intended purpose, what the software can perform and achieve in practice[215]. Potentially, in a situation where there is a conflict between the two intended purposes, a manufacturer could circumvent the MDR to cut costs and red tape. Still, one may argue that an attempt to establish the degree of the intended purpose of what would classify as a medical device and what would not, has been established by the "manual of borderline and classification in the Community regulatory framework for medical devices"[216] which provides a non-exhaustive list of devices that are considered as borderline medical devices.

Also, the CJEU case law does not provide more clarity on the classification of a medical device to detangle the intended purpose phenomena. Throughout the years, the CJEU has interpreted differently from time to time what may constitute a medical device under the regulatory regime. For instance, in Brain Products GmbH a device for recording human brain waves was found by the Court not to be a medical device because the manufacturer of the device did not intend for it to have a medical purpose[217]. Yet, in 2017 the CJEU in the Snitem case ruled that "software, of which at least one of the functions makes it possible to use patient-specific data for the purposes of detecting contraindications, drug interactions and excessive doses, is, in respect of that function, a medical device" within the meaning of the MDD[218,219]. The preliminary ruling suggests a shift in the interpretation of the intended purpose and, thus, that of a medical device under the regulation, proposing that the court will increasingly emphasise the function of the device while it will consider the intended purpose rather briskly[220]. The Court's shift also suggests that the function of the software or device is as important as the intended purpose and that both explicit and implicit intended purposes should be aligned.

---

[215] Paul Quinn, 'The EU Commission's Risky Choice for a Non-Risk Based Strategy on Assessment of Medical Devices' (2017) 33 Computer Law and Security Review 361.

[216] EU Commission, 'Manual on Borderline and Classification in the Community Regulatory Framework for Medical Devices (Version 1.22)', vol 22 (2019).

[217] Jessica Morley, Luciano Floridi and Ben Goldacre, 'The Poor Performance of Apps Assessing Skin Cancer Risk' (2020) 368 BMJ m428 <http://www.bmj.com/lookup/doi/10.1136/bmj.m428> accessed 11 February 2020.

[218] 'Are Wearables Medical Devices Requiring a CE-Mark in the EU? | Covington Digital Health' <https://www.covingtondigitalhealth.com/2019/01/are-wearables-medical-devices-requiring-a-ce-mark-in-the-eu/> accessed 26 May 2021.

[219] *Judgment of the Court (Fourth Chamber) of 7 December 2017 Syndicat national de l'industrie des technologies médicales (Snitem) and Philips France v Premier ministre and Ministre des Affaires sociales et de la Santé Request for a preliminary ruling from the Conseil d'État (France) Reference for a preliminary ruling — Medical devices — Directive 93/42/EEC — Scope — 'Medical device' — CE marking — National legislation making drug prescription assistance software subject to a certification proce…* (2017) C-329/16.

[220] Adrian Thorogood and others, 'Genetic Database Software as Medical Devices' (2018) 39 Human Mutation 1702.

Furthermore, more and more borderline digital health technologies are entering the EU market. For example, mHealth devices linked to wellness may potentially be used in a shady way. For instance, consider a digital wellness device (a sleep-tracing application) that is not officially used in a treatment regime prescribed by a health professional, but is integrated in a de facto manner by a patient as an aid to their treatment[221]. Therefore, one of the main questions that should be answered is: how and to what extent do digital health technologies, which do not qualify as medical devices under the MDR, ensure its user data privacy and security? The MDR remains silent in this respect.

Consequently, correctly qualifying digital health technology as a medical device is a fundamental step before launching a digital health technology in the EU market. Should such digital health technology fall under the medical device definition, it would require greater regulatory scrutiny and an assessment of safety and security standards. If digital health technology does not fall under the MDR definition of a medical device, it would allow digital health technology to circulate freely in the EU market. The underlying risks are clear. Even with a clear-cut regulatory regime, such borderline digital health technologies may create a tidal wave where such digital health technologies will be marketed directly to the patient. This is especially relevant with all incoming "well-being" applications and devices.

Finally, while the EU establishes safeguards to protect consumers under the EU product liability regime, in case of applications or devices falling under the MDR, the implications are not clear cut. The Boston Scientific case, which dealt with the liability of defective cardiovascular defibrillators and pacemaker devices, was judged on the grounds of the EU Product Liability Directive, while the product itself, being a medical device, had to undergo regulatory approval under MDD, which allowed it to be placed onto the EU market in the first place[222]. The former MDD, and now the MDR, did not address and has not addressed any liability issues when it comes to the failure of medical devices. The MDR simply guides the manufacturer to the relevant provisions of the Product Liability Directive as a means of coordinating the complex inter-regulatory health IoE environment. Lastly, not correctly qualifying health technology would bring about fines and administrative proceedings, but also could significantly affect an individual's rights to quality medical care, safety, security, and health.

4.4.5 Establishing Mechanisms of Legal Coordination and Co-requisite Approach for Digital Health Technologies

[221] Quinn (n 216).

[222] Judgment of the Court (Fourth Chamber) of 5 March 2015 Boston Scientific Medizintechnik GmbH v AOK Sachsen-Anhalt Requests for a preliminary ruling from the Bundesgerichtshof Reference for a preliminary ruling — Consumer protection — Liability for dama.

Some authors have already addressed how secondary mechanisms of legal coordination in regulation can prevent threats and risks of fragmentation due to complex interaction between several converging EU regulations[223]. Thus, in this section, we argue that the MDR establishes mechanisms of legal coordination and co-requisite approach of digital health technologies qualifying as medical devices to ensure data protection and privacy. We further observe that such mechanisms of legal coordination and co-requisite approach established under the MDR could be applied as industry best practices for digital health technologies that do not qualify as medical devices.

To start with, we note that from the perspective of the GDPR, digital health technologies which process personal data must conform with the GDPR, yet not all such digital health technologies must comply with the MDR compliance regime. For instance, an application that allows individuals to voluntarily trace their sleep quality will be required to comply with the GDPR, but would not fall under the MDR regime, since it would not be considered a medical device. Yet, in cases where digital health technologies, such as sensors or remote health monitoring technologies, have developed into legitimate medical devices that collect data concerning health, GDPR becomes a legal co-requisite for MDR compliance. Such a legal co-requisite requirement is also reflected in Articles 109 and 110 of the MDR. Articles 109 and 110 of the MDR require specific attention to compliance with data protection and patient confidentiality regulations of all parties involved in the manufacturing of a medical device. We further note that the MDR does not establish how compliance with the GDPR for medical devices should be achieved, the MDR simply directs the manufacturers of the medical devices to the GDPR for guidance, as part of its harmonised approach to end-user (consumer) safety and security.

Also, the MDR compliance process requires that all medical devices conform with the quality, safety, and security requirements set out in the MDR. Such conformity is required not only for medical devices before (pre-market conformity) they enter the EU market but also throughout their lifetime on the EU market (post-market conformity).

Additionally, the MDR establishes that the quality management of medical devices must also consider all security and safety standards that may apply to a specific case using harmonised standards (art.8) and common specifications (art. 9), set out in Annex I of the MDR. The same annexe lists the General Safety and Performance Requirements ("GSPR"). In essence, the use of compliance standards such as ISO 27001, IEC 60601, IEC 62304, and ISO 14971 for qualifying medical devices give the "presumption" of compliance with the MDR.

[223] Pagallo, 'The Legal Challenges of Big data: Putting Secondary Rules First in the Field of EU Data Protection' (n 151).

Similarly, the existing Network and Information Security (henceforth, the "NIS Directive") Directive and the proposed NIS2 Directive together with the Cybersecurity Act (henceforth, the "CA") become legal co-requisites for medical device compliance with the MDR, as digital health technologies that qualify as medical devices would fall under both regulatory regimes.

Before explaining how the MDR enshrines this legal coordination mechanism between different legislations we should briefly discuss the relevance of NIS, NIS2, and the CA in the digital health technology context. In this respect, the NIS2 establishes greater capabilities when compared to NIS in terms of more stringent supervision measures, enforcement, increased EU-level cooperation, strengthened security requirements and accountability for the Operators of Essential Services (henceforth, the "OES"), which also includes the healthcare sector[224]. NIS coverage in the healthcare sector includes recommendations at the national level for hospitals to establish cybersecurity strategies in different industries and implement state-of-the-art cybersecurity measures and policymakers to promote collaboration on cybersecurity across the EU and in the public-private sector[225]. The NIS2 also includes recommendations for manufacturers of IoT devices, including manufacturers of digital health devices which incorporate sensors, software, wearables and so on. In the digital health sector, recommendations for manufacturers extend to the incorporation of security into existing quality assurance systems, involving third-party testing, consideration to apply medical device regulation to critical infrastructure and involving healthcare organisations throughout the entire device lifecycle[226].

The CA closes the cybersecurity regulatory circle by establishing a European base framework for the cybersecurity certification of ICT products, covering manufacturers of digital and electronic medical devices that use ICTs such as sensors, wearables, or remote monitoring technologies. While it does not provide a single certification framework for digital health technologies or medical devices, it gives baseline recommendations for the certifying bodies when drafting cybersecurity certification schemes.

With this background in mind, we can now identify the above-mentioned legal coordination mechanisms from the analysis of the MDR itself. Specifically, Annex I of the MDR provides a set of harmonised minimum safety and performance requirements that reiterate the requirements that would apply to medical devices[227]. In fact, upon a closer analysis of Annex I rules, IT security

---

[224] ENISA, Good Practices for Security of Internet of Things in the Context of Smart Manufacturing (2018) <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot>.

[225] Dimitra Liveri, Anna Sarri and Christina Skouloudi, Security and Resilience in EHealth (2015) <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/ehealth_sec/security-and-resilience-in-ehealth-infrastructures-and-services>.

[226] ENISA (n 225).

[227] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing

requirements may be found in section 17.4. and 23.4(a) and 23.4(b) of Annex I, while operation security is referred to in sections 14.1., 14.2, 17.1, and information security in section 1 of the MDR Annex 1 and section 17.2 of the same Annex. In terms of IT security and information security, the focus lies with the safety and effectiveness of the devices where any risks are "weighed against the benefits to the patients" [228], which are "compatible with a high level of protection of health and safety, considering state-of-the-art" [229] (section 1). It should be observed that "risks related to data and systems security are specifically mentioned within the scope of the risk management process to avoid any misunderstanding that a separate process would be needed to manage security risks related to medical devices"[230].

Likewise, section 4(a) of Annex 1 of the MDR ensures privacy and data protection through secure design and manufacturing practices and includes several measures for such protection. Such measures vary from protection against unauthorised access (sections 17.4 and 18.8), the establishment of risk control measures (sec. 4), to the identification of threats and vulnerabilities (sec.3b). Also, Annex I further requires the establishment of minimum IT security measure requirements in sections 17.4 and 14.5. All these measures are supported via a regular update of the state-of-the-art technologies as mentioned in sections 1.4 and 17.2., which seem to provide extensive guidance on cybersecurity requirements for digital medical devices. Similarly, the Medical Device Coordination Group (henceforth, the "MDCG") guidance on cybersecurity for medical devices (named the "MDCG 2019-16") confirms the relationship between the different legislations applicable to digital health technologies qualifying as medical devices[231].The MDCG also acknowledges that, amongst the many novelties, the MDR enhances the legislator's focus "on ensuring that devices placed on the EU market are fit for the new technological challenges linked to cybersecurity risks"[232] in the digital world. Furthermore, we should also mention that the risk assessment exercise is key when ensuring the high level of data protection and privacy for digital health technologies that qualify as medical devices must be considered throughout the lifecycle of such devices[233].

Bringing Europe's digital health technology regulatory regime in line with the technological advancements and consumer expectations is complicated. The MDR does so through establishing a mechanism of legal coordination, to prevent the fragmentation of the legal system in the complex

---

Council Directives 90/385/EEC and 93/42/EE.

[228] Medical Device Coordination Group, 'Guidance on Cybersecurity in Medical Devices - Artical 103 of Regulation (EU)2017/745' [2019] Medical Device 1 <https://ec.europa.eu/docsroom/documents/41863>.

[229] ibid.

[230] Medical Device Coordination Group, 'Guidance on Cybersecurity for Medical Devices' [2019] MDCG 2019-16 Rev.1 1 <https://ec.europa.eu/docsroom/documents/38941>.

[231] The European Commission, 'MDCG 2021-05 Guidance on Standardisation for Medical Devices.Pdf' (2021).

[232] Medical Device Coordination Group (n 231).

[233] Medical Device Coordination Group (n 229).

digital health technology environment. The main tool of this coordination mechanism is the co-requisite approach of the MDR uniting privacy, cybersecurity, and digital health technologies under one roof. The co-engineered design of the MDR could also be a recipe for reducing privacy and data protection risks for digital health technologies. It must be clarified, however, that in no way does the MDR attempt to override the regulatory requirements set out in the GDPR, NIS, NIS2, or the CA. Rather, through the legal coordination mechanism established in the MDR, the regulation requires specific attention to certain aspects of data protection and privacy, while the requirements that are not specifically mentioned in the MDR remain subject to other legislation[234]. At the same time, the coordination mechanism allows for streamlined compliance for the manufacturers of digital health technologies that qualify as medical devices, becoming a win-win solution for both patients that can use safe and secure devices and manufacturers of medical devices.

Consequently, the established legal coordination and co-requisite mechanisms in the MDR play a fundamental role, not only in terms of data protection and privacy but also, in the prevention of the fragmentation of the legal system in the complex digital health technology environment. Even more so, the legal coordination and co-requisite mechanisms of the MDR could serve as an inspiration for digital health technologies that do not qualify as medical devices for the protection of personal data and privacy. In this sense, the observed legal coordination and co-requisite mechanisms set out the minimum data protection and privacy measures to be implemented when developing digital health technologies. As a final note, this section did not address the proposed EU AI Act's and the MDR's interaction, which is discussed in detail in Chapter 6.

4.5 Conclusive Remarks

This chapter presented an in-depth discussion regarding the conceptualisation of the complex regulatory regime of digital health technologies in the European Union. In general, the chapter explored how and to what extent this complex regulatory regime on big data is applicable to digital health technologies without hindering an individual's right to privacy and the right to health in health emergency situations. In particular, the chapter found that the dawn of the digital age brought a fundamental shift from the right to privacy to the right of data and thus, towards the protection of individual (personal) data. Such a shift expanded the scope of the rights connected to privacy and individual personality rights, which may be threatened by the collection or processing of personal data.

[234] ibid.

Based on the above premise, the chapter delved into analysing the importance of the notions of personal data and data concerning health in a big data and digital health technology context. Regarding the notion of personal data, the chapter argued that, even though the General Data Protection Regulation does not include the notion of big data in its text, big data is covered under the scope of the GDPR. The legal analysis of the notion of personal data as contained in Article 4 of the GDPR established that big data is covered under the GDPR due to the broad definition of personal data in the GDPR and its surrounding interpretation. It should be observed in this respect that data, including personal data, is a context-driven notion. Therefore, while the same data might in one context be considered as personal, in another it might not. For example, anonymised social network data would not be considered personal; however, if it were combined with another data source, such data could become personal due to inferences that could be made with data analytics. In essence, Article 4 of the GDPR provides an all-encompassing context-based concept of personal data that also includes big data. Regarding the notion of data concerning health enshrined in the GDPR, it was observed that the GDPR's interpretation of the notion, like the notion of personal data, considers big data in the same way as in the context of personal data. Yet, considering the sensitivity of data concerning health, the processing of such data requires an additional layer of protection regardless of the volume of data processed.

Considering that the fundamental right to privacy and data protection requires protection at both the European and national levels, the chapter further explored the role of the DPIA as an instrument to ensure data protection in the context of digital health technologies. In the context of healthcare and digital health technologies, it should be observed that Article 35 of the GDPR incorporates a requirement for a Data Protection Impact Assessment to be carried out in cases where the use of new technologies may result in a high risk to the rights or freedoms of natural persons. It has been observed that Article 35 GDPR requires a DPIA to be carried for data that will be processed using new technologies, taking into account the scope of the processing, i.e., the volume of data (referred to as "large-scale" data processing) and the envisaged impact it would have on the protection of personal data, ensuring that big data processing is also covered by the requirement for a DPIA. Based on this, in 2017 the Working Party 29 published Guidelines on DPIA, determining whether the processing is "likely to results in a high risk" for the purposes of GDPR. The chapter analysed the guidelines and carried out research on the transposition of the above-mentioned guidelines by five selected Member States, namely, Italy, Malta, Lithuania, UK, and France. The results are summarised in Table 3. Results of the analysis on processing which is "likely to result in a high risk" above.

In this regard, the research found that the transposition of the guidelines differs greatly in the above Member States due to the non-mandatory nature of the guidelines. The analysis also led to the conclusion that there is a lack of a common European understanding and approach not only to DPIA but also to big data.

Delving deeper into the complex regulatory regime in the context of big data and digital health technologies led to the analysis of the medical devices' regulatory regime from the perspective of the GDPR, considering that health technologies that process personal data must conform with the GDPR, yet not all such digital health technologies must comply with the MDR compliance regime. For instance, an application that allows individuals to voluntary trace their sleep quality will be required to comply with the GDPR, but would not fall under the MDR regime, since it would not be considered a medical device. Yet, in cases where digital health technologies, such as sensors or remote health monitoring technologies, have developed into legitimate medical devices that collect data concerning health, the GDPR becomes a legal co-requisite for MDR compliance. In fact, the legal analysis of the MDR revealed that the legal coordination mechanism is enshrined in Articles 109 and 110 of the MDR, by making GDPR compliance a legal co-requisite to the MDR. It was further observed that the MDR does not establish how compliance with the GDPR for medical devices should be achieved, it simply directs the manufacturers of the medical devices to the GDPR for guidance, as part of its harmonised approach to end-user(consumer) safety and security. Nonetheless, the MDR establishes a legal coordination mechanism between vertical and horizontal regulations at the EU level that does not only provide protection in terms of data protection and privacy, but also facilitates the prevention of the fragmentation of the legal system in the complex digital health technology environment.

5 Regulating Public Healthcare Emergencies: Balancing the EU Citizen's Rights to Privacy, Data Protection, and the Right to Public Health

This chapter of the thesis scrutinises the legal and regulatory background of an extraordinary event, the Covid-19 pandemic. The research on the topic of the thesis started in early November 2019, before the start of the Covid-19 pandemic. Yet, the unexpected outbreak of the Covid-19 pandemic and the healthcare technologies deployed in the three short years due to this pandemic, became are a "favourable" event that allowed the research to be exemplified, specifically in the European scenario. Thus, providing the required depth of thought for the research. While the Covid-19 pandemic allowed the research to observe the events and the regulatory approaches to public health emergencies management in real time, it should be observed that at the EU level, public healthcare emergency management has existed for decades. The regulatory field at the Union level for such crisis management was limited to directives which in themselves had limited purposes and gave EU limited powers for managing public health emergencies and crises at a supranational level. The Covid-19 pandemic changed this to an extent as will be observed in this chapter.

Therefore, in this chapter the focus will be on the transnational nature of the Covid-19 pandemic in the informational society as observed by Pagallo[235], and on the EU's attempt to deal with such a crisis at a supranational level. The following sections will analyse the attempt to manage the Covid-19 crisis at the Union level and the limits of such an endeavour through several legislative means. Such legislative attempts will shed light on how the existing regulatory privacy and data protection regimes played an important role in the deployment of the Covid-19 technologies. It will also address how ad hoc guidelines and EU's approach ensured the protection of the fundamental rights to privacy and data protection in the Covid-19 emergency.

Two case studies will then be presented: one focuses on the European vaccination certificates, while the other focuses on contact tracing applications, as Europe's response to pandemic management and its implementation by selected Member States. The final section of this chapter examines the latest EU regulatory responses to public health threats, the proposal for a regulation on Serious Cross-Border Threats to Health.

5.1 The Current State of Play: Using Digital Technologies in Healthcare Emergencies. Balancing Fundamental Rights with Limited Competences and National Diversions

[235] Pagallo, 'Sovereigns, Viruses, and the Law: The Normative Challenges of Pandemic in Today's Information Societies' (n 139).

The protection of life and health are fundamental rights enshrined not only in the Charter of Fundamental Rights of the European Union, but also in the national constitutions of the Member States of the European Union. Constitutions of the various Member States enshrine these rights differently, each with its limitations and exceptions. For instance, Article 32 of the Italian Constitution enshrines the right to health as a fundamental right of the individual and, also, as a collective interest. Similarly, Article 19 of the Constitution of Lithuania enshrines protection to life, while Article 53 enshrines the notion that the "State shall take care of people's health"[236]. These fundamental rights are the basis of legitimisation of any subordinate sources for the protection of such rights, allowing both the EU, to the extent its competencies allow, and the Member States to implement measures for the protection of such rights.

In the European Union context, public health is a shared competence between the EU and the Member States, enshrined in Article 4(2)(k) of the TFEU. It is one of the areas where the EU has limited powers. Further, Article 168 of the TFEU, which deals with public health, is the legal basis for most of the EU's initiatives in the digital health sector.

While the EU aims to establish a high level of human health protection, the Union's actions in the healthcare space can only complement Member States' national policies. Given that public health is a shared competency of the EU, the possibility of harmonising laws in public health is limited. Such limitation of competencies, which ultimately led to divergent approaches in the Member States, can be illustrated well by the Covid-19 crisis.

Furthermore, the right to private life and data protection enshrined both, in the European fundamental rights documentation and Member States' constitutions, are also not to be considered as absolute rights[237]. For instance, balancing the right to private life enshrined in Article 8 of the ECHR should be done by striking a fair balance "between the competing interests of the individual and of the community as a whole"[238]. While the von Hannover case was not decided in the case of an emergency, it allows us to perceive the limits of personal freedoms and liberties against those of the community.

Additionally, the ECHR Article 52 establishes a clause limiting the rights and freedoms recognised by the Charter. Similarly, the case law above refers to such limitations, which, as the ECtHR has observed, should be subject to the principle of proportionality (established in the same Article 52) and where there is a necessity to protect rights of persons or achieve the Union's objectives. It could

[236] 'Constitution of the Republic of Lithuania (Adopted by Citizens of the Republic of Lithuania in the Referendum of 25 October 1992)'.

[237] As for, example, noted by the Court of Justice of the European Union in Eifert case: "The right to the protection of personal data is not, however, an absolute right, but must be considered in relation to its function in society." In joined Cases C-92/09 and C-93/09 Volker und Markus Schecke GbR (C-92/09) and. Hartmut Eifert (C-93/09) v Land Hessen [*2010*] *ECR* I-*11063 (para. 48)*

[238] Von Hannover v Germany (no 2) [GC] - 40660/08 and 60641/08 Judgment 722012 [GC].

be argued that both von Hannover and the earlier Eifert cases reinforced the interpretation of the freedoms to privacy and personal data that was followed by the European Union in its response to the Covid-19 crisis, i.e., the (potential) limitation of such rights considering the higher objective of the protection of the European community from the spread of the Covid-19 virus.

With this background in mind, the following two sections of the thesis examine instances of how the Covid-19 pandemic was managed by the European Union using digital health technologies while ensuring the balance of the personal fundamental freedoms against those of the society at large.

5.2 A Taxonomy of the Covid-19 Applications

As discussed earlier in the work, within the scope of public healthcare emergencies lie big data technologies used in combating and preventing the spread of various diseases and pandemics. The use of the Covid-19 pandemic as one of the case studies for the work was only natural. The research on public health emergency management in healthcare began in November 2019, just before the outbreak of the Covid-19 pandemic, which we then lived through, survived, and experienced first-hand.

Furthermore, due to the interconnectivity of the digital world, the majority of the Covid-19 technologies deployed at a European level in the prevention and management of the said pandemic were highly available for analysis and inspection. This is due to the open access provided by both the European Union and some of the Member States, academia, and private entities. Observations were made by scholars that "the emergence of these syndromic surveillance systems which sought to enhance the surveillance and reporting of pandemic risk in the late 20th century also facilitated a novel broader turn in practices of surveillance towards the development of new digital surveillance technologies, and the implementation of accelerated data processing capacities to address contingent pandemic risks"[239].

The case study of the Covid-19 technologies focuses on the analysis of privacy and data protection aspects (particularly, the GDPR) of technologies used in the collection, processing and sharing of data, and the fundamental rights implications to the rights of health and the right to privacy. In order to establish a structure to the Covid-19 case study, we have broadly grouped the Covid-19 applications into:

1. First-generation Covid-19 applications which may be further classified into:
    a. InfoApps, such as the WHO application, which provides updated statistical

[239] Gerybaite and Aurucci (n 54).

information on Covid-19 symptoms, number of cases and so on;

b. Exposure Notification Applications, such as "Immuni" used in Italy.

c. Quarantine applications, which encompass all surveillance tools of individuals in quarantine which are primarily used by law enforcement; and

2. Second-generation Covid-19 applications which may be further categorised into:

a. Proofs of Vaccination. Such technologies may otherwise be known as "Immunity Passports" or "green certificates"[240], such as the one used in Estonia during the pandemic; and may also include;

b. Other mHealth applications, such as wearable devices which, in their original design may not have been designed to assist with tracking or the prevention of pandemics, but due to various software updates introduced (e.g., introducing additional functionalities in smart watches) by the developers, may nevertheless assist in the prevention or monitoring of the pandemic or its symptoms[241].

It has been observed that the "risks associated with the outbreaks of epidemics or pandemics do not only affect global public health or worldwide economy, but also due to the proliferation of digitalisation and the data available bring about unforeseen risks associated to the use of the so-called big data tools within healthcare when trying to prevent, predict, manage or treat arising pandemics"[242]. Also, "due to the diverse sources and types of big data used in epidemiology, the privacy risks associated with the use of such big data emerge from the notion of big data itself and the features attributable, the 3Vs: volume, velocity, and variety"[243]. From privacy and data protection standpoints, some authors identify that big data raises three key privacy issues:

1. The risk on inadvertent disclosure of personally identifying information[244];

2. "increasing dimensionality of data which makes it difficult to determine if a data set is sufficiently deidentified to prevent deductive disclosure of personally identifying information; and

3. the challenge of identifying and maintaining standards of ethical research in the face of emerging technologies that may shift the generally accepted norms regarding privacy"[245].

---

[240] Note: such a name might be misleading as "digital green certificates" within the EU context are usually used to represent a certificate that certain electricity is generated from renewable energy sources.

[241] 'Wearable Tech Is Being Used to Stem Outbreaks of COVID-19 | World Economic Forum' <https://www.weforum.org/agenda/2020/05/elderly-home-wearables-contact-tracing-apple-google> accessed 28 October 2020.

[242] Gerybaite and Aurucci (n 54).

[243] ibid.

[244] Mooney and Pejaver (n 113).

[245] ibid.

By definition, any type of contact tracing requires the giving up some part of personal information by the data subject, thus, it is crucial to address the above privacy issues in specific case-to-case studies against the utility trade-off of such applications.

Thus, the analysis of the data protection, privacy, and fundamental rights implications of the ICT technologies used in the prevention, tracing and monitoring of the Covid-19 pandemic will be done through an analysis of different tools used in real-world Covid-19 management with concluding remarks following at the end of the chapter. We note that the work focuses on the analysis of exposure notification and quarantine applications while excluding InfoApps. Such a decision for the analysis was made as InfoApps are purely information tools that provide information to users without the need to process any personal data, thus falling outside the scope of the research which focuses on data protection and security aspects. InfoApps are briefly addressed at the beginning of the next section.

5.3 Crisis Management with Digital Technologies: First-generation Covid-19 applications

5.3.1 Information Applications

Various information-providing applications are used for the management of public emergencies. In some cases, commonly used consumer platforms such as Facebook may become InfoApps through the introduction of additional functionalities in their platforms. Consider, for example, Facebook's info tool in the case of natural disasters such as earthquakes and tornadoes which provided up-to-date information to its users on security or Facebook's additional functionality on health-related information (with respect to Covid-19 pandemic). At an international level, informational applications such as the WHO application has been used to provide its users with updated statistical information on Covid-19 symptoms, the number of cases and other related pandemic information. Such applications, in most cases, do not process personal or personal sensitive data therefore fall outside the discussion of this thesis.

5.3.2 The Case of Contact-Tracing Technologies

Exposure notification applications or contact-tracing applications are technologies covering the contact tracing of infected individuals and can be used interchangeably. Contact-tracing technologies may also be considered as the first-generation technologies used and deployed to place a bridle on the Covid-19 outbreak. While parts of Europe were deep into the second wave of the Covid-19, healthcare researchers were working on forestalling future outbreaks and developing

first-generation applications that would minimise the necessity for lockdowns of entire nation-states.

In Europe, various contact-tracing and exposure notification applications took off as the first response promoting the prevention of the spread the Covid-19 virus. Amongst these applications, exposure notification applications have been by far the most prominently used ones in Europe. Out of 27 EU Member States, more than 20 have deployed exposure notification applications, as noted in the EU Commission[246]. The reason for such a spread is simple: proper isolation and quarantine may reduce transmission of diseases.

Exposure notification applications are not new to healthcare professionals in managing various pandemics. While the current form of exposure notification technology takes the shape of mobile applications, earlier versions used simple SMS and GPS mechanisms. For instance, contact-tracing and exposure notification technologies assisted in managing the Zika outbreak[247].

Yet, the success of such exposure notification technologies is debatable. Examples of the same technology used in Sierra Leone or Kenya had significant limitations regarding pandemic containment, as it exposed the drawbacks of cell phone data being used for exposure notification[248]. Nonetheless, knowing and understanding the drawbacks of the first attempts led to significant improvements in exposure notification technologies that, as we will uncover, were used in Europe during the Covid-19 pandemic[249].

The distribution of exposure notification applications as first-generation pandemic targeting technologies has brought about the need to limit the overarching effects of these instruments. Namely, their impact on the fundamental freedoms, such as the right to data protection, the right to privacy, the right to health, and public safety. The rights enshrined in the European Treaties, such as the right of free movement of persons and the right of association were also affected by the deployment of these technologies, limiting not only personal freedoms but also affecting group privacy rights, as discussed by Pagallo[250].

While authors tend to discuss the legal side of the problems arising, only a few authors have analysed the technology's efforts to limit the unwanted effects of such applications. Therefore, we

---

[246] European Commission, 'Mobile Applications to Support Contact Tracing in the EU's Fight against COVID-19 Progress Reporting June 2020' (2020).

[247] Jennifer Salerno and others, 'Untangling the Ethical Intersection of Epidemiology, Human Subjects Research, and Public Health' (2019) 34 Annals of Epidemiology 1.

[248] Susan L Erikson, 'Cell Phones ≠ Self and Other Problems with Big data Detection and Containment during Epidemics' (2018) 32 Medical Anthropology Quarterly 315 </pmc/articles/PMC6175342/?report=abstract> accessed 18 September 2020.

[249] Amy Wesolowski and others, 'Connecting Mobility to Infectious Diseases: The Promise and Limits of Mobile Phone Data' (2016) 214 Journal of Infectious Diseases S414 <https://academic.oup.com/jid/article/214/suppl_4/S414/2527905> accessed 18 September 2020.

[250] Pagallo, 'Sovereigns, Viruses, and the Law: The Normative Challenges of Pandemic in Today's Information Societies' (n 8).

take a multidisciplinary approach and link the two different sides of the same coin. Through the Covid-19 technology examples, the thesis uncovers the impact of big data-based digital technologies on fundamental rights to health, public safety, privacy, the right to data protection, and the rights enshrined in the European treaties such as the right of free movement and association.

5.3.2.1 Contact-Tracing Technologies: Balancing the Right to Data Protection and Public Safety During the Covid-19 Pandemic

Philosophical concepts often presume that the world consists of cooperating and benevolent individuals who are willing to voluntarily support each other and society[251]. In the digital world, such cooperation can take the shape of, for instance, the sharing of their personal data for Covid-19 pandemic management purposes. Yet, in practice matters are different. A survey on the Covid-19 pandemic in the EU and fundamental rights implications which focused on contact-tracing applications found that 23% of the responders were not willing to share their personal data with the public administration[252]. Even more, 41% of the respondents of the same survey did not wish to share personal data with private enterprises. Also, only 45% of the citizens trusted their governments, as stressed by an OECD study[253]. In the context of the Covid-19 pandemic, such numbers are even more striking due to the state of emergency and the uncertainty it causes.

Moreover, the notion of public safety is arguably related to the notion of the common good. Common good may refer to those qualities, whether cultural or institutional, that members of a particular community have in common, and all agree to care for[254]. Thus, in today's world, common good may be transposed into sets of common values that different societies agree to protect.

---

[251] For example, John Rawls in his works refers to "reasonable citizens who want to live in a society in which they can cooperate with their fellow citizens on terms that are acceptable to all [...and where…] they are willing to propose and abide by mutually acceptable rules, given the assurance that others will also do so" 'John Rawls (Stanford Encyclopedia of Philosophy)' <https://plato.stanford.edu/entries/rawls/> accessed 29 July 2022.. For further reading, Audard, C. (2007). John Rawls (1st ed.). Routledge. https://doi.org/10.4324/9781315712109
In addition, Benkler in Wealth of Networks notes that in the so-called networked information economy, "new and important cooperative and coordinate action carried out through radically distributed, nonmarket mechanisms that do not depend on proprietary strategies—plays a much greater role <…> than in the industrial information economy. The catalyst for this change is the happenstance of the fabrication technology of computation, and its ripple effects throughout the technologies of communication and storage." The nonmarket mechanisms through "large-scale cooperative efforts—peer production of information, knowledge, and culture <…> based in the networked environment and applied to anything that the many individuals connected to it can imagine. Its outputs, in turn, are not treated as exclusive property." Individuals therefore "are using their newly expanded practical freedom to act and cooperate with others in ways that improve the practiced experience of democracy, justice and development, a critical culture, and community" ibid..

[252] European Union Agency for Fundamental Rights, "Coronavirus pandemic in the EU- Fundamental Rights Implications: with a focus on contact-tracing apps."

[253] 'Trust in Government - OECD' <https://www.oecd.org/gov/trust-in-government.htm> accessed 4 January 2021.

[254] 'The Common Good (Stanford Encyclopedia of Philosophy)' <https://plato.stanford.edu/entries/common-good/> accessed 22 September 2020.

Inherently, public safety, public health, data protection, and privacy may be defined as some of the common good values protected in the European Union.

In addition, as we already observed above in the chapter, public safety itself may entail many diverse perspectives depending on cultural, societal, and economic circumstances that surround a certain community. From a more practical perspective, public safety may be referred to as emergency preparedness, i.e., healthcare emergency management of the Covid-19 pandemic. Concerning the Covid-19 pandemic and its toll on the EU, we should observe that public safety does not only refer to the well-being of a community, through the guaranteeing of health, but in a broader sense also refers to the overall return to the 'normal' everyday functioning of the society from a socio-economic perspective.

In this context, national states and sovereign governments play a crucial role in protecting the common good, not only in ordinary circumstances but also in times of crisis. In scenarios such as the Covid-19 pandemic, governments and sovereigns are entitled to use the so-called powers of emergency to protect the common good and ensure public safety[255].

Nonetheless, regarding such emergency powers invested by the people into national governments and sovereigns, we observe that traditional mechanisms used in times of crisis risk being misleading or even short-sighted. Different authors argue that we should be paying attention to the informational features of Covid-19 both in terms of the epistemological status of the pandemic and the normative counterparts to gain a clearer understanding of the traditional mechanisms of emergency powers and measures, its rights, and restrictions[256].

In healthcare emergencies, the "sheer urgency of containing an exponentially spreading virus has thrown it into relief the always present issue of ability of the GDPR to strike a balance between conflicting interests" [257], such as the right to health and the right to privacy, eventually becoming a controversial issue. We can observe that the controversy lies, on the one hand with the "increasing demand from public authorities and private entities for tighter measures that involve the massive processing of different types of personal data to contain and mitigate the effects of the virus"[258]. On the other hand, the ""wrong" belief that increased surveillance and unlimited limitations to the right of protection of personal data is "a necessary evil""[259] to preserve lives also contributed to such controversy.

[255] Gerybaite (n 73).
[256] Pagallo, 'Sovereigns, Viruses, and the Law: The Normative Challenges of Pandemic in Today's Information Societies' (n 8).
[257] Gerybaite and Aurucci (n 54).
[258] ibid n 9.
[259] Francesco Paolo Micozzi, 'Le Tecnologie, La Protezione Dei Dati e l'emergenza Coronavirus: Rapporto Tra Il Possibile e Il Legalmente Consentito' (2020) 2 BioLaw Journal 1.

With the explosion of the use of mobile exposure notification applications during the early months of 2020 in Europe, the European Data Protection Board had no time to rest. Due to the growing concerns of mass surveillance, potential breaches to privacy, and data protection, the EDPB had to react and provide guidance to the Member States on the processing of personal data to fight the Covid-19 virus[260]. The EDPB held its first meeting with a focus on the Covid-19 crisis on 3rd April 2020, wherein it discussed the necessary guidance and opinions to be provided concerning the personal data processing in the Covid-19 pandemic. In the weeks following the initial meeting, the EDPB published two noteworthy guidelines for the Covid-19 fight: "Guidelines on the Use of Location Data and Contact Tracing Apps in the Context of the COVID-19 Outbreak"[261], and the "Guidelines on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the COVID-19 Outbreak"[262]. The first guidelines provided essential guidance on the definition of data concerning health, the processing for the purposes of scientific research, the legal basis for such processing, its exemptions, and the rights of the data subjects about the Covid-19 pandemic. The latter guidance instead specifically focused on the use of location data and exposure notification applications.

In this context, we should note that the EU data protection regime was designed to be as flexible as possible to achieve both targets – limit the spread of the virus and protect fundamental human rights and freedoms. It is also worth mentioning that the EDPB "considers that data and technology used to help fight the Covid-19 should be used to empower, rather than to control, stigmatise, or repress individuals"[263]. Furthermore, while data and technology can support the crisis management measures, they have intrinsic limitations and can merely leverage the effectiveness of other public health measures[264,265].

The EDPB's approach to contact tracing technologies focuses on the general principles of necessity, effectiveness, and proportionality, otherwise known as data-management principles. The

[260] 'Contact-Tracing Apps in Poland A New World for Data Privacy'.

[261] European Data Protection Board, 'Guidelines 04/2020 on the Use of Location Data and Contact-Tracing Tools in the Context of the COVID-19 Outbreak' (2020).

[262] European Data Protection Board, 'Guidelines 03/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the COVID-19 Outbreak' (2020) <https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en>.

[263] 'Statement on the Processing of Personal Data in the Context of the COVID-19 Outbreak | European Data Protection Board' <https://edpb.europa.eu/news/news/2020/statement-processing-personal-data-context-covid-19-outbreak_en> accessed 24 March 2020.

[264] European Data Protection Board, 'Guidelines 04/2020 on the Use of Location Data and Contact-Tracing Apps in the Context of the COVID-19 Outbreak', 2020.

[265] As interestingly observed by Beqiraj and others in the context of Covid-19 and contact-tracing technologies: "*GDPR <…> reflects the right-duty framework of a social contract. Also, the Rule of Law values emphasis on "a social consensus on the acceptable level of conditional data collection for public health safety and the appropriate methods for collection must be addressed head-on in preparation for the next pandemic*". Julinda Beqiraj and others, 'IEAI White Paper "Rule of Law, Legitimacy and Effective COVID-19 Control Technologies" Institute for Ethics in Artificial Intelligence' [2022] EAI White Paper Series <https://www.ieai.sot.tum.de/ieai-white-paper-series-rule-of-law

proportionality concerning the exposure notification apps and geolocation apps entail that such apps should only be implemented for two specific purposes. Firstly, to support the response to the pandemic through the modelling of the spread of the virus, for instance, location data. Secondly, to notify individuals of their exposure to Covid-19, for instance, via exposure notification. The necessity in terms of the GDPR concerning exposure notification technologies refers to the necessity for the performance of tasks considered to be in the public interest as underlined in Article 6.1(e) of the GDPR.

The adoption of contact-tracing technologies in the EU to contain and combat the epidemiological emergency of the Covid-19 virus, in a highly complex context, was an unprecedented challenge for the Member States' governments. For contact-tracing applications to be successful and effective, they had to be downloaded, installed, and used by the majority of the population of a single Member State where such technology was implemented. For instance, in Italy, for the contact-tracing application "Immuni" to be successful, it was calculated that it had to be downloaded and used by at least 60% of the population with smartphones.

We can observe that Europe's attempt to achieve the goal of managing the spread of Covid-19 by incentivising the sharing of data is achieved through ensuring that the public trusts the Covid-19 measures implemented. In fact, it should be observed that the public's trust is a legitimator of the Covid-19-related control measures that are deployed. Particularly in the example of contact-tracing applications, it can be observed that such "efficacy of technology depends on user subscription (such as contact tracing technology), then citizen compliance is central to the effective exercise of these powers"[266,267].

Also, our trust in the technology is tested through challenging the way we communicate and interact with each other, and our civic responsibility towards each other. Several factors contribute towards the success of achieving such a goal. First, we should discuss trust in technologies[268]. With the

[266] Julinda Beqiraj and others, 'IEAI White Paper "Rule of Law, Legitimacy and Effective COVID-19 Control Technologies" Institute for Ethics in Artificial Intelligence' [2022] EAI White Paper Series <https://www.ieai.sot.tum.de/ieai-white-paper-series-rule-of-law/> accessed 28 July 2022.

[267] While the thesis does not delve deeper into the trust issue of the use of technologies, especially in scenarios such as the Covid-19 pandemic, several papers have been published discussing the relationship between trust in technologies and the rule of law that may ensure legitimate use of such technologies, and how the rule of law can cultivate trust. Interestingly, as observed by Beqiraj and others: the "*adherence to principles of the Rule of Law encourages State transparency and accountability, which help to promote positive trust outcome*", while the lack of information and transparency cultivates distrust. For further, in-depth analysis please see, Julinda Beqiraj and others, 'IEAI White Paper "Rule of Law, Legitimacy and Effective COVID-19 Control Technologies" Institute for Ethics in Artificial Intelligence' [2022] EAI White Paper Series <https://www.ieai.sot.tum.de/ieai-white-paper-series-rule-of-law

[268] As observed by both L.Floridi, the "*problematic nature of trust in technology becomes evident with the dissemination of ICTs and the subsequent information revolution, with which artefacts cease to be used mainly to perform physical and fatiguing tasks and begin to be deployed to execute also intellectual work*". Moreover, as also discussed by M. Taddeo it is "important to discuss the occurrence of trust in digital environments, the nature of trust in technology and the relation between trust, technology, and design" Mariarosaria Taddeo, 'Trust in Technology: A

digital world looming, a mental shift can be observed. Focus is shifting from questioning the legality of digital technologies (whether, for instance, an application is legal) to trustworthiness of such technologies. Thus, trust in technological solutions is one of the key elements to achieve such a goal yet promoting it in such a complex environment as pandemics with exacerbated psychological and social effects on the population is no easy task.

In this regard, diverse "trustworthiness methodologies" are to be employed to ensure a successful deployment of contact-tracing technologies. For instance, the Italian contact-tracing application "Immuni" employs several of such trustworthiness methodologies. First, we can observe how trustworthiness is ensured through transparent disclosure of information during the lifecycle of "Immuni". Public disclosure of the functionality and security features of the application, the publication of the documentation, and the underlying code of the application for public access from the inception of the technology throughout its lifetime, is fundamental in a crisis scenario[269].

Second, ensuring trust through voluntary use. "Immuni" was used voluntarily as enshrined in Article 6(1) of the Legislative Decree 28 of 30 April 2020, which ensured that individuals would retain the freedom of choice[270]. Third, ensuring trust through regulatory assessment. Such assessment for the protection of personal data takes the share of a DPIA, required under Article 35 of GDPR. Usually, a DPIA must be carried out where personal data is processed "using new technologies" and considering the "nature, scope, and purposes of the processing", where such processing "is likely to result in a high risk to the rights and freedoms of any natural person"[271]. The publishing of the DPIA report is not yet obligatory under the GDPR, considering the nature of the application and its potential implications to fundamental human rights, the DPIA of "Immuni" was made available for full transparency purposes[272].

Finally, since the efficiency of contact-tracing technologies depends on many factors, some of which were addressed above. However, it is fundamental that contact tracing form part of a comprehensive public health strategy for combating the pandemic. While exposure notification and isolation of contacts are paramount in the fight against the spread of viruses, it is likewise necessary to deploy algorithms for learning from data responsibly with due respect to regulatory compliance

---

Distinctive and a Problematic Relation' (2010) 23 Knowledge, Technology & Policy 2010 23:3 283 <https://link.springer.com/article/10.1007/s12130-010-9113-9> accessed 29 July 2022.;

[269] 'Immuni-Documentation/README.Md at Master · Immuni-Application/Immuni-Documentation · GitHub' <https://github.com/immuni-application/immuni-documentation/blob/master/README.md#analytics> accessed 21 September 2020.

[270] Il Presidente Della Repubblica, "Decreto Legge 30 Aprile 2020, n.28" (2020), https://www.gazzettaufficiale.it/eli/id/2020/04/30/20G00046/sg.

[271] 'Data Protection | European Commission' (n 184).

[272] 'Valutazione d'impatto Sulla Protezione Dei Dati Personali Presentata Dal Garante Privacy' <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9357972> accessed 17 July 2020.

and fundamental freedoms[273,274]. Thus, contact-tracing technologies should not be considered as the "holy grail" solution for combating Covid-19.

5.3.3 Surveillance Applications of Individuals in Quarantine

Who is to say when contact tracing becomes a full-on nation-wide surveillance operation? The line between contact tracing and surveillance is a thin one. On the one hand, tracing of contacts of infectious people is a tool that assists the management of pandemics. On the other hand, if the power given to the state, sovereign, or public administration is unlimited, nation-wide surveillance scenarios may occur. In this section of the thesis, we will address another type of technology used by states to prevent and manage the Covid-19 pandemic, namely the surveillance technologies that states deploy on individuals in quarantine.

Such applications are often used by the law enforcement to ensure that infected individuals remain in mandatory quarantine. For example, South Korea deployed the repurposed technologies already used by their tax authorities for public health purposes to manage the infection rates. The specific tools used for surveillance by South Korean authorities were the movements of the credit and debit card transactions which allowed the exact locations of individuals to be seen, phone location logs, and the use of the South Korea's network of surveillance. For example, cameras in restaurants, train stations and so on[275]. South Korea's example of surveillance to manage the Covid-19 crisis is of a particular interest as it portrays an establishment of a large, intra-ministerial, public and private sector cooperated, nation-wide surveillance system, with data collected and processed from both public and private sectors, and various government departments to ensure the most accurate individual surveillance possible for the prevention of the Covid-19 pandemic. For example, Hong Kong had introduced tracing wristbands for persons in obligatory quarantine.

Closer to home, in Europe, Poland had introduced the 3rd Covid Act which obliged telecommunication providers to disclose the localisation data of persons in mandatory quarantine, upon request from the Ministry of Digitalisation of Poland[276]. Reports started showing up that the

---

[273] Marcello Ienca and Effy Vayena, 'On the Responsible Use of Digital Data to Tackle the COVID-19 Pandemic' (2020) 26 Nature Medicine 463 <https://doi.org/10.1038/s41591-020-0832-5> accessed 28 September 2020.

[274] As observed by Beqiraj and others: "<…> *the benefits which the contact tracing apps in the containment of COVID can be balanced with the need to ensure that there is no threat to the personal information and the right to privacy and digital security of users. This balance can be maintained by ensuring that the data collected during the period is used strictly to ensure containment of the virus; through lawful, fair, and transparent use of the data; and controlled access to the data, as indicated in the GDPR*". Julinda Beqiraj and others, 'IEAI White Paper "Rule of Law, Legitimacy and Effective COVID-19 Control Technologies" Institute for Ethics in Artificial Intelligence' [2022] EAI White Paper Series <https://www.ieai.sot.tum.de/ieai-white-paper-series-rule-of-law

[275] 'Tech Tent: Can We Learn about Coronavirus-Tracing from South Korea? - BBC News' <https://www.bbc.com/news/technology-52681464> accessed 4 November 2020.

[276] 2020 FRA - European Union Agency For Fundamental Rights- Coronavirus Pandemic in The EU - Fundamental Rights Implications (Poland), Bulletin #1, 'Coronavirus Pandemic in The EU - Fundamental Rights Implications

Prime Minister of Poland obliged telecom operators to provide further localisation information on individuals remaining in quarantine, which had no justification[277]. In fact, under the 2nd Covid Act, Poland has also launched "Kwarantanna Domowa" an application for subjects in mandatory 14-day quarantine, which "uses geolocation and face recognition technology to ensure that relevant people are quarantined"[278]. In this respect, it should be observed that the Polish State places an obligation on a person who has been put in obligatory quarantine to download the application (unless such a person is exempt if she/he does not own a smartphone) and undergo a self-identification process. Instead of receiving on-site check ups by the police, an individual in quarantine would, from time to time, receive an SMS with a request that she/he has a time frame of 20 minutes to perform the self-identification task and confirm his/her location. The task would require the said individual to allow the application to track his/her GPS coordinates and a person's identity through a real-time selfie check. The GPS coordinates of the person are compared with the ones held in the central server and they must match the location declared for quarantine, while the selfie photograph taken is compared by a facial recognition technology to confirm the identity of the person in quarantine.

Failure to conform with the time-to-time requirements of the application, would constitute a signal for the Polish police task force to directly (i.e., in person) verify whether users of the application comply with the quarantine requirements. The use of the application for the person in quarantine is obligatory and in case of non-compliance a person may face an administrative fine of up to approximately EUR 6,600 or, depending on the circumstances, legal consequences may arise under the Code of Misdemeanours or, in most serious cases, the Polish Criminal Code[279]. The last two measures depend on the severity and relate to the Codes' articles on non-compliance with bans and orders with regard to the prevention of infectious diseases, whilst the last measures relate to the action that put people at risk of infection in terms of the Polish Criminal Code.

From a technical point of view, we assessed the said mobile applications' vulnerabilities in terms of privacy and data protection. In this regard, the application Kwaratina Domowa was tested through ImmuniWeb's mobile application security test. The mobile security test methodology follows the OWASP top ten pen testing which allows mobile applications to be tested and identifies vulnerabilities as outlined in Annex A. The OWASP pen test is designed to identify, safely exploit, and help address these vulnerabilities, so that any weaknesses discovered can be quickly addressed.

(Poland)' (2020) <https://en.wikipedia.org/wiki/2020_coronavirus_pandemic_in_Belgium>.

[277] 'Statement on Restrictions on Data Subject Rights in Connection to the State of Emergency 1 in Member States' <https://net.jogtar.hu/jogszabaly?docid=a2000179.kor>.

[278] Magdalena Brewczyńska, 'Contact Tracing Apps in Poland A New World for Data Privacy', vol 2 (2020).

[279] Magdalena Brewczynska, 'The Polish Government's Actions to Fight Covid-19: A Critical Look at the "Selfie Application" and Direct Access to Location Data' (2020) 6 European Data Protection Law Review (EDPL) <https://heinonline.org/HOL/Page?handle=hein.journals/edpl6&id=314&div=&collection=> accessed 12 February 2021.

This allowed the research to establish potential privacy and data protection issues in the application. OWASP top ten methodology is highly deployed within the research and the industry and the use of ImmuniWeb's tool was chosen due to its availability for research purposes.

The results of such testing showcased that the application requires access not only to the location (GPS) of the mobile phone and the camera (to ensure face recognition of individuals in quarantine), which is understandable due to the nature of the application and its function. In fact, the application also requires access to other phone functionalities such as: external storage of the device (for example, SD card) in a write or read mode; microphone, i.e., the mobile application can record audio using the phone's microphone; contact list (in read or write mode); finally, the phone function (i.e., the application can answer phone calls, or access/modify phone state)[280].

In fact, authors have already debated that such an application raises concerns as regards the compliance with the right to privacy and protection of personal data as enshrined in the ECHR, as well as the Polish Constitution itself[281]. It has been observed by researchers that, as to the legal basis for the processing of personal data by the application in the terms and conditions of the use of the application, there is an inconsistency between the declared legal basis for the processing of personal data stemming from the Covid-19 Act vis-à-vis the legal basis for processing in terms of Article 9(2)(i) of the GDPR.

If one were to evaluate the above-mentioned technical aspects of the application in terms of its compliance with the GDPR, one could not overlook the fact that the Polish surveillance measures almost ignores the data minimisation and purpose limitation principles as set out in Articles 5(1)(b) and 5(1)(c) of GDPR. In this respect, the GDPR requires data to be collected only for specific, explicit, and legitimate purposes and, that the data collection is adequate and, even more importantly, "relevant and limited to what is necessary in relation to the purposes for which they are processed"[282]. Considering that the Polish application not only received unnecessary access, but also through such access would be able to collect data from the device storage, contacts, microphone and all the phones' functions it is doubtful that the principles set in Articles 5(1)(b) and 5(1)(c) of GDPR could be said to be complied with.

Also, we should address how the data minimisation principle is tackled by the application creators. As mentioned above, though the application claims to only collect GPS data and photos of the user, it nonetheless has unnecessary and unauthorised access to the potential collection of data within the

---

[280] For the full report please refer to Annex A: ImmuniWeb, 'Summary of Mobile Application Security Test OWASP Mobile Top 10-Kwarantanna Domowa' (2020) which provides an analysis on the application's mobile security features in line with The Open Web Application Security Project ("OWASP") Top 10 provided methodology.

[281] Brewczynska (n 280).

[282] Bart Custers and others, 'Lists of Ethical, Legal, Societal and Economic Issues of Big data Technologies' [2018] SSRN Electronic Journal 1.

SD storage of the smartphone, record audio using phone's microphone, contact list and so on as mentioned above.

Furthermore, the application indicates that user data will be retained for "six years, except for images which are deleted when the user deactivates the account"[283]. In comparison, in other European applications the data retention period is only 14 days. Such a lemgthy data retention period is not only worrisome, but also questions the proportionality of the measure itself. Considering that the terms and conditions of the application only include the necessary legal basis for the processing of GPS location data and photos of individuals, the application clearly does not have the necessary legal basis for access (and potential collection) to all the other personal data on a user's smartphone. One may attempt to argue that such access to a smartphone's data is required for the proper functioning of the application itself, however this is not the case with the application at hand. It is acceptable practice in the industry by both developers of the applications and their legal teams to limit the access to the smartphone data to only the necessary data points for the proper functioning of such an application, to protect unauthorised access to the user's data and to ensure data protection and privacy for the users of the apps. In fact, one may argue that it may be considered negligent that neither the designers of the application nor the Polish government confronted the unauthorised access to users' data. In the same vein, concerns may be raised as to what extent the proportionality of the measures as required by the GDPR has been assessed. One may doubt to what extent the DPIA has been carried out with respect to the potential risks to users of such an application. It is safe to conclude that the data minimisation principle and the principle of proportionality enshrined in the GDPR have not only not been addressed but also seem to have been left out of the considerations.

Beyond GDPR concerns, we must also address the fact that the application collects and processes location data of the application users. In this situation we must assess the rules applicable to such processing in terms of the e-Privacy Directive. The said directive requires data to be anonymised for processing and should it not be so, there must be explicit consent from the user. Article 15 of the e-Privacy Directive provides for exemptions if such are "necessary, appropriate, and proportionate within a democratic society to safeguard national security (i.e., State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system <...>"[284]. The above-mentioned list does not explicitly include public health, yet one may argue that public health falls within the broader

[283] Brewczynska (n 280).

[284] OJ L 201 The European Parliament, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) 2002 37.

notions of 'public security' as mentioned in Article 15(1) of the directive. To this extent, arguments have been made that including public health within the notion of public security would be a rather far-fetched argument for the exemption to apply[285]. Similar legal concerns were addressed in the report issued by the EU's Fundamental Rights Agency that acknowledged legal challenges with the obligation imposed by the Covid Acts to provide localisation data to the Ministry of Digitalisation of phones belonging to persons subject to quarantine[286]. Interestingly, another legal challenge that came out from the report was the fact that while the police can use its statutory measures to ensure that people remain in mandatory quarantine, however, such measures exclude mass surveillance measures. While police may require access to the content of communication (as one of the statutory measures), such a measure excludes the metadata of such communications, i.e., the localisation data of the mobile devices. One may argue that the Polish application could fall under the umbrella of mass surveillance measures as implemented by the Polish government for the sole purpose of tracking and surveilling persons in obligatory quarantine which, due to the pandemic, amounts to a significant portion of its population. The FRA's report also seems to lead the way to challenging the legal grounds of processing location data as it may be contested it would not satisfy the exemption contained in the e-Privacy Directive[287]. Clearly, due to the lack of transparency, particularly, with respect to solutions used to protect personal data collected by the application, "Kwarantanna Domowa" faced scrutiny not only from the public but also from the Polish Ombudsman who has requested an official opinion from the Polish Office for Personal Data Protection.

5.4 Crisis Management with Digital Technologies: Second Generation Technologies

5.4.1 The Deployment of Proofs of Vaccinations in the EU

With the Covid-19 pandemic being part of the new normal in early 2021, economies shrinking due to global lockdowns, newly approved vaccinations administered to health workers, the EU and its Member States entered a new stage in the pandemic crisis management. With infection numbers stable[288], opening borders and facilitating the growth of economies while managing the risk of increased the Covid-19 cases became challenging. While vaccinations seemed to provide a way out, these had to be administered throughout the whole European continent to ensure their efficacy. Mandatory vaccinations and certificates in Europe against Covid-19 became part of public debate with the stakeholders involved. In this regard, the ECtHR has also been invoked to provide its

[285] Brewczynska (n 280).
[286] FRA - European Union Agency For Fundamental Rights- Coronavirus Pandemic in The EU - Fundamental Rights Implications (Poland), Bulletin #1 (n 277).
[287] ibid.
[288] One can also explore the question of what can be considered stability in times of crisis

decisions and judgements in several cases relating to Covid-19. In the period of the Covid-19 vaccine certifications, the ECtHR has considered the case of a French lecturer claiming that by creating and imposing an obligatory vaccination passport system, French "laws amounted to a discriminatory interference with the right to respect for private life"[289]. In another case, a French national lodged a complaint with the ECtHR that the French State failed to fulfil its positive obligation to manage the Covid-19 pandemic[290]. Yet, the ECtHR in both cases found that the cases were inadmissible[291].

In the first case, the inadmissibility basis was the fact the Court was not asked to determine whether France failed to fulfil its positive obligations "to take appropriate steps to safeguard the lives of those within its jurisdiction"[292] and to protect their physical integrity. The Court observed in the first instance, that the applicant failed to prove that "the measures taken by the French State to curb the Covid-19 virus among the whole population of France" [293] or that such measures had a personal effect on the applicant, particularly when the application is done under Article 34 of the Convention (individual application), the applicant must prove that he or she was directly affected by the measures implemented. The Court reiterated that it has not recognised actio popularis, i.e., "that applicants cannot complain about a provision of domestic law, a domestic practice or public acts simply because they appear to contravene the European Convention"[294].

In the second case of Zambrano, the inadmissibility of the case was due to several facts. In this case, however, the Court declared that the applicant failed to exhaust all domestic remedies applicable when contesting the Covid-19 vaccination certificates and the fact that the applicant's actions "amounted to an abuse of the right of individual application" as enshrined in the Convention[295]. In both cases the Court refrained from delving into the substance of the claims as to whether the French State's actions amounted to discriminatory interference with individual freedoms protected by the Convention.

Vaccine certificates are a competence of the Member States, issued according to their national laws, while sharing data about who is vaccinated and with what types of vaccines, rarely leaves the borders of a particular Member State. In the Covid-19 pandemic, that transcends national borders, the EU's response was crucial to ensure a timely pandemic response. A divergent approach within

[289] 'Decision Zambrano v. France - Application Which Was Challenging the French "Health Pass"' <https://hudoc.echr.coe.int/eng-press#%7B%22itemid%22:[%22003-7145978-9686694%22]%7D> accessed 13 December 2021.

[290] 'Le Mailloux v. France, HUDOC - European Court of Human Rights' <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:[%22003-6873639-9217565%22]%7D> accessed 13 December 2021.

[291] European Court of Human Rights, 'Factsheet- COVID-19 Health Crisis' (2021).

[292] ibid.

[293] ibid.

[294] 'Le Mailloux v. France, HUDOC - European Court of Human Rights' (n 291).

[295] 'Decision Zambrano v. France - Application Which Was Challenging the French "Health Pass"' (n 290).

Europe on the Covid-19 vaccination and their certificates brought with it the risk of slowing down the reopening of mobility and economies. Thus, a discussion took place on the single European approach to the Covid-19 vaccine certifications.

The first step to the proofs of vaccinations was taken in January 2021, when the Member States, with the support of the European Commission, adopted the EU e-Health Network guidelines "establishing an EU-wide interoperability framework for proofs of vaccinations"[296]. These guidelines were "based on Carte Jaune, the paper format of the vaccination certificate"[297], but they explicitly dealt with the digital format of the vaccination certificate. The guidelines provide an interoperable trust framework for digital vaccination certificates based on: "1. Simplicity, which would allow the certificate schemes to be established in both paper or digital formats; 2. Flexibility and compatibility with existing national solutions; 3. Rigorous protection of personal data; and 4. Stepwise approach, with agreement among the Member States at each step of the way"[298].

We should note that the guidelines are technical in their nature and establish three primary data elements for proofs of vaccinations. First, a minimum data set that captures "basic information required for the certificate"[299]. Such information included "three elements which are a person's identifications, vaccination information, and certificate metadata"[300]. Moreover, vaccination certificates also included personal data, including name, surname, identification number, sex, and date of birth"[301].

Another element concerned the specific information as regards to the vaccination and included "disease or agent targeted, vaccine, vaccine medicinal product, marketing authorisation holder (e.g., Pfizer BioNTech), batch/lot number, date of vaccination, the centre of administration of vaccination, country of vaccination, future dates"[302] for vaccination. Together with the certificate's metadata, which included the "certificate issuing entity, certificate identifier, certificate validity date, these datasets would be interoperable and shareable between the Member States"[303].

The eHealth Network guidelines established that "the vaccination certificate system should be designed in such a way that the data subject can control the use of the certificate data"[304]. How such controls were to be ensured remained "unclear as the guidelines only refer to the GDPR data

[296] Gerybaite (n 73).
[297] ibid.
[298] ibid.
[299] ibid.
[300] ibid.
[301] ibid.
[302] ibid.
[303] ibid.
[304] ibid.

minimisation principle for proofs of vaccinations, while other GDPR related issues such as automated processing are not addressed"[305].

It can be observed that until June 2021, an EU-wide framework for proof of vaccinations did not exist. The proofs of vaccinations existed in digital and paper formats either in the format of Carte Jaune, a WHO approved vaccination certificate for certain vaccines, or in any other shape or form as decided by the Member States individually. This changed with the adoption of a proposal for the regulation on the so-called "Digital Green Certificate" (henceforth, the "DGC") which was published in March 2021 and adopted following a special legislative procedure on 15th June 2021[306].

Several aspects should be noted in this respect. The DGC is highly based on the e-Health Network guidelines adopted by the Member States. Yet, while the guidelines aimed at creating an interoperable vaccination certificate, the regulation aim is special. The DGC regulation aimed to allow EU citizens to exercise the right of free movement within the EU during the Covid-19 pandemic which would "allow EU citizens and their family members exercising their right to free movement to demonstrate that they fulfil public health requirements imposed, in compliance with EU law"[307]. In other words, the guidelines establish a "technological solution to achieve the EU's aim to facilitate the free movement of persons during pandemic times"[308].

Second, notwithstanding a noble aim, the adopted regulation has received criticism. With "vaccination tourism" being "a reality in some of the European countries, the criticism was that the introduction of DGCs could facilitate greater free movement restrictions for EU citizens who have received non-EMA approved vaccines"[309,310].

It can also be observed "that a vaccination de facto generates proof of vaccination"[311]. Depending on where the vaccination was administered, "such proof may take a form of an immunity passport, opportunity passport or a similar shape, carrying different consequences for the vaccinated individual or groups of individuals"[312].

From a legal standpoint, the adopted regulation places great focus on privacy and personal data protection when compared to the e-Health Network guidelines, both at individual and group privacy levels. It can be observed that while data from various Covid-19 vaccinations could be necessary to

[305] ibid.
[306] ibid.
[307] Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic 2021 1.
[308] Gerybaite (n 73).
[309] Ashok Kumar Verma and Sadguru Prakash, 'The Commission against the Internal Market and EU Citizens Rights: Trying to Shoot down Sputnik with the "Digital Green Certificate"?' (2020) 09 7352.
[310] Gerybaite (n 73).
[311] ibid.
[312] ibid.

locate the infected part of the population, such data could also form part of the policymaking[313]. For instance, vaccination data could be used to assist a state's government in pandemic management at a public level. At the individual level, however "false-positive results of Covid-19"[314] tests might lead to a government-ordained quarantine. It should be observed that "policies predicated on antibody testing, such as immunity passports, are not only impractical given these current gaps in knowledge and technical limitations, but also pose considerable equitable and legal concerns, even if such limitations are rectified"[315].

Since all such data would fall under the GDPR definition of personal sensitive data an additional level of protection is required. Processing of personal sensitive data (data concerning health to be exact) under "GDPR is prohibited, unless such collection and processing fall under Article 9(2) GDPR exemptions discussed in Chapter 4"[316]. Article 9(2)(i) includes one of such exemptions. The said article postulates that in cases of public interest of public health, such as protecting against serious cross-border threats to health based on Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subjects, the processing of data concerning health is permitted[317,318].

In this respect, the GDPR enshrines exact data protection-related issues concerning the issuance of vaccination certificates. For instance, "Article 9 of the regulation addresses the legal basis for the processing of data related to health (personal sensitive data), data minimisation principle, purpose limitation, and storage limitation principle"[319]. Thus, the regulation enshrines requirements regarding processing and purposes of processing personal. For example, concerning the data minimisation principle, the Digital Green Certificates provided an exhaustive list of personal data required for such certification, guaranteeing that no unnecessary personal data is processed.

5.4.2 A Case Study of the Estonian "Immunity Passport" Application

The pilot application of the "Estonian immunity passport allowed users to manage their data about medical certificates issued with respect to the RNA (RT-PCR) test results and antibody detection (immunological) test results issued by doctors on Covid-19"[320]. The said application, "developed by

[313] ibid.
[314] ibid.
[315] ibid.
[316] ibid.
[317] ibid.
[318] The European Parliament and The Council Regulation (EU) 2016/679 of the European Parliament and 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 (n 9).
[319] Gerybaite (n 73).
[320] ibid.

a public-private sector collaboration, the Estonian government and two of the well-known tech companies in Estonia"[321], acted as a support technology for the Covid-19 management.

The legal basis for the processing of the user's data takes place with the consent of the user in terms of the GDPR 9(2)(a)[322]. While most national contact-tracing applications used the derogation provided under Article 9(2)(i) GDPR for the processing of personal sensitive data, for immunity passports, the Estonian government went in another direction and provided users with the freedom to choose whether to share or not share their personal data.

The application includes several security and privacy features specifically designed to protect data starting from access to the application, data capture, data access and sharing to data analysis. For example, the 'ImmunityPassport' "manages a central database in the AWS cloud environment where the recorded test results are stored with the source code of the entire application and infrastructure"[323] made open source on GitHub. One may question whether such storage of personal data on an Amazon cloud server is compatible with the current EU regulatory regime, particularly, considering the recent Schrems II decision.

The application also claims that the user is the "sole owner of their data" [324], who "can share their data on the application"[325] with employers, institutions, or anyone else via a QR code, validated on a minute basis. Open access to such personal "sensitive data expires after an hour"[326] which ensures that the data is protected against the unauthorised sharing of sensitive health data.

User registration, log in, and authentication takes places through a 'magic-link' system where one-time login links are sent to the user. The links contain an authentication code that can be exchanged for a secure token used for future requests. Such 'magic links' are one-time links with expiration after the first login. The data collected by the application includes data on the birth, sex, full address of the use and data is only communicated over secure SSL connections.

The application assigns roles and gives permissions to a limited number of parties, including medical professionals with a recognised role who performed the tests on a patient which provides a greater amount of trust that the records of the patient are correct. Additionally, any data analysis is performed only on anonymised data sets, and only by authorised personnel. In this regard, the developers do not only ensure data protection through the means of technology but also employ ISO standards on organisational measures for the protection of PII (consider ISO 27701), i.e., focusing on the people in the organisation who have access to the PII and who are authorised to process the

[321] ibid.
[322] 'ImmunityPassport: FAQ.' <https://www.immunitypassport.co/faq> accessed 16 November 2020.
[323] ibid.
[324] ibid.
[325] ibid.
[326] ibid.

data. The developers further elaborated that it is not possible to use other data of the patient to deanonymise test result data as there is no link between the two in either direction[327]. Date of birth is converted to age while the address of the user is converted to region to further prevent statistical deanonymisation of result data[328].

Deanonymisation techniques used in this example may be effective when personal data is taken in separate categories (such as age, residence and so on), however, several studies have shown that once such different data categories are combined, data analytic tools may re-identify a particular individual. In fact, recent studies have shown that one only requires 15 demographic attributes to re-identify one individual[329]. It can be observed that a comprehensive regulatory regime and guidance should have been issued for the introduction of proofs of vaccinations in terms of data protection. While the EU provided such guidance, it fell short of addressing all underlying data protection and privacy concerns.

5.4.3 Other mHealth Technologies

This section of the thesis mentions other technologies used to manage the Covid-19 pandemic. For instance, smart watches that updated their functionality to include software features such as oxygen measurement. A fascinating point of contention between the previously mentioned tools and the mHealth example of such technologies is the public nature of contact-tracing apps versus the private nature of smart watches' introduced technology and the private sector capitalisation on the Covid-19 pandemic.

The discussed and analysed technologies deployed by the public sector, while not totally fault-free, were developed and deployed on the basis of strict data protection and privacy by design and by default principles, trying to avoid any sort of traceability of private individuals and their personal data. While a smart watch is a useful device, questions might be raised as to the ethics of capitalisation on the public health emergency such as Covid-19 to entice persons to disclose their health-related data, which would profit private entities vis-à-vis public health goals.

5.5 Incentivising the Use of Data in the Covid-19 Pandemic Scenario

The incentivisation of the use and sharing of data is not an entirely new phenomenon. As observed by Benkler, in the information economy, "freedom of action for individuals who wish to produce

[327] 'GitHub - Cov-Clear/Backend: Backend Service API' <https://github.com/cov-clear/backend> accessed 16 November 2020.

[328] ibid.

[329] Luc Rocher, Julien M Hendrickx and Yves Alexandre de Montjoye, 'Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models' (2019) 10 Nature Communications 1 <https://doi.org/10.1038/s41467-019-10933-3> accessed 8 February 2021.

information, knowledge, and culture is being systematically curtailed in order to secure the economic returns demanded by the manufacturers"[330]. Such incentivisation of data, while observed first from an economic perspective, where non-market forces, i.e., consumers or users of technologies, play the prominent role in the information economy, can also be translated into the example of Covid-19 pandemic and data, particularly health data sharing in the times of crisis. In the situation of the Covid-19 pandemic, contact-tracing applications, as the one analysed in the previous sections of the thesis, where the same consumer-generated data were used to achieve public health purposes, specifically, maintaining the spread of a virus. Contrarily to Benkler's information economy observations, in the situation of the Covid-19 pandemic scenario, the use of data draws away from benefiting private entities in the "information economy", such data is instead deployed for the benefit of everyone, i.e., the society at large. It can be observed that the use of data here is supported by the arguments of public good and public safety. While the goal is noble at its core, we must also acknowledge that such sharing of data in the instance of contact tracing application and other the Covid-19 pandemic management applications was incentivised by one's civic responsibility rather than economic incentives[331]. In fact, while the sharing of data in the Covid-19 scenario was based on the public good argument, the adoption of such contact tracing applications took more time to be (and has also been scrutinised by the public in detail) adopted by society at large[332].

Finally, we should consider that we live in a world where surveillance is based on the principle "for your safety and our curiosity". Therefore, the incentivisation of the use and sharing of health data through digital contact-tracing technologies used in times of public health emergencies, such as the Covid-19 pandemic, as an attempt to manage the spread of Covid-19 challenges the cultural and social fabric of the society, the way we communicate and interact with each other and our civic responsibility towards each other.

5.6 Responding to Crisis via Crisis Preparedness: EU's Proposal for the Regulation on Serious Cross-Border Threats to Health

[330] Yochai Benkler, *The Wealth of Networks : How Social Production Transforms Markets and Freedom* (New Haven [Conn] : Yale University Press, [2006]©2006 2006).

[331] For example, government backed cash-back schemes that require authorities to access personal data regarding individual's financial transactions are usually more successful and take less time to implement. The sharing of personal sensitive data is facilitated by a sort of "reward" of a cash-back scheme. The author of the thesis does not support a "reward" mechanism for sharing data. The example is used solely for illustrative purposes.

[332] Leonie Kahnbach and others, 'Quality and Adoption of COVID-19 Tracing Apps and Recommendations for Development: Systematic Interdisciplinary Review of European Apps' (2021) 23 J Med Internet Res 2021;23(6):e27989 https://www.jmir.org/2021/6/e27989 e27989 <https://www.jmir.org/2021/6/e27989> accessed 18 July 2022.

A final examination in this chapter focuses on the EU Commission's latest response to the Covid-19 and the named proposal for the Regulation on Serious Cross-Border Threats to Health. The said proposal was published late in 2020 as a response to strengthen and create a better EU health union, as well as ensure that the EU has the means to address healthcare threats that lie beyond national borders[333].

The proposal can be described as a building block for the Union's health crisis management as it would allow the Union to address new healthcare threats more rapidly at the EU level for a coordinated response. Such a coordinated response is necessary considering that the Member States, during the Covid-19 pandemic, have adopted uncoordinated and at times competitive national responses to the crisis, often based on "distinctive risk analysis frameworks, with little regard for the scientific and management advice provided by the EU, notably its dedicated legal framework for action on cross-border health threats"[334]. The newly proposed regulatory framework would also ensure that errors that occurred during the Covid-19 crisis management are not repeated. The said regulation would amend the currently applicable "Decision No. 1082/2013/EU on serious cross-border threats to health"[335]. Currently, decision 1082/2013/EU provides a "limited legal framework for EU level coordination"[336] focusing on the exchange of information and cooperation within the Health Security Committee[337]. In this respect, the proposed regulation would complement several already existing EU measures in the field of crisis management, including the creation of the "future European Health Data Space by encouraging innovation and research, facilitating the sharing of information (including real-world evidence), and supporting the development of a Union-level IT infrastructure for epidemiological surveillance"[338].

The legal basis for the regulation lies with Article 168(5) of the TFEU and Article 2(5) stipulates the required support for the Union to act and supplement national measures without superseding Members States' competencies in healthcare. The main tools the regulation proposes are the establishment of "an EU health crisis and pandemic preparedness plan, complemented by national plans and transparent reporting of capacities; strengthened, integrated surveillance systems; enhanced risk assessment for health threats; increased power to enforce a coordinated response at

[333] European Commission Proposal for a Regulation of the European Parliament and the Council on serious cross-border threats to health and repealing Decision No 1082/2013/EU (n 13).
[334] Alberto Alemanno, 'The European Response to CoviD-19: From Regulatory Emulation to Regulatory Coordination?' (2020) 11 European Journal of Risk Regulation 307 <https://doi.org/10.1017/err.2020.44> accessed 25 January 2021.
[335] European Commission Proposal for a Regulation of the European Parliament and the Council on serious cross-border threats to health and repealing Decision No 1082/2013/EU (n 13).
[336] ibid.
[337] ibid.
[338] ibid.

EU level through the Health Security Committee; and an improved mechanism for recognition of and response to public health emergencies"[339].

While during the first wave of the Covid-19 pandemic the Member States implemented their own measures to combat Covid-19, the second Covid-19 wave exposed the fact that collaboration at the EU level is taking longer than anticipated and that the established mechanisms are not sufficient to quickly address health threats[340]. For instance, the ECDC "did not have sufficient critical epidemiological information on the spread of the virus in Europe"[341]. While we saw some collaboration at the EU level, such as the establishment of the interoperability gateway for the contact-tracing technologies, such technologies form only part of the crisis management plan.

Nonetheless the EU's response to health crisis preparedness, the proposed regulation has received criticism. Some authors note that the proposal for the regulation only tweaks pre-existing mechanisms of the decision on cross-border health threats rather than strengthening and establishing a sound EU health union[342].

While the thesis in a previous chapter discussed that healthcare emergencies are highly context-related, establishing a definition of a public health emergency would increase accountability regarding actions taken, to both the Member States and Union citizens. In this regard, the regulation does provide a common notion for a definition of a "serious cross-border threat to health" in Article 3(7)[343]. Such serious cross-border health threats are those that are life-threatening, which spread or can spread across "national borders of Member States', and which may necessitate a coordinated response at the Union level to ensure a high level of human health" [344] protection. It can thus be observed that the proposed notion is an attempt of the Union in establishing basic requirements for the recognition of health emergencies, at least at the European level. The establishment of a common notion of a cross-border health threat as proposed by the regulation would allow actions across the Member States and the Union to be streamlined in case of cross-border health threats. Simultaneously, establishing a common notion of a serious cross-border threat to health at the

---

[339] ibid.

[340] Anne Laure Beaussier and Lydie Cabane, 'Strengthening the EU's Response Capacity to Health Emergencies: Insights from EU Crisis Management Mechanisms' (2020) 11 European Journal of Risk Regulation 808 <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/strengthening-the-eus-response-capacity-to-health-emergencies-insights-from-eu-crisis-management-mechanisms/A8DCBA29DCC1985BB0CDAB50AEC38127> accessed 10 December 2021.

[341] ibid.

[342] Hannah VAN KOLFSCHOOTEN, 'EU Coordination of Serious Cross-Border Threats to Health: The Implications for Protection of Informed Consent in National Pandemic Policies' (2019) 10 European Journal of Risk Regulation 635 <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/eu-coordination-of-serious-crossborder-threats-to-health-the-implications-for-protection-of-informed-consent-in-national-pandemic-policies/91117A9FE70273CCCD00F3203719BD98> accessed 25 October 2021.

[343] European Commission Proposal for a Regulation of the European Parliament and the Council on serious cross-border threats to health and repealing Decision No 1082/2013/EU (n 13).

[344] ibid.

European level would also entail a wide range of legal effects for the Member States, such as aligning domestic legislation in line with the new notion.

On the technological side, the proposed regulation pays attention to how various digital health technologies can be used to assist in a public health crisis. For instance, one of the subject matters of the proposed regulation is the establishment of integrated surveillance, disease monitoring, and contact tracing systems as part of the larger EU epidemiological surveillance measures. Contact tracing in terms of the proposed regulation refers to measures implemented "to trace persons who have been exposed to a source of a serious cross-border threat to health, and who are in danger of developing or have developed a disease, through manual or other technological means"[345]. In line with the digitalisation of the EU, the ECDC will be tasked with the creation of a digital surveillance platform that would "enable the automated collection of surveillance and laboratory data (as per the proposal), make use of information from electronic health records, media monitoring, and apply artificial intelligence for data validation, analysis, and automated reporting, and allow for the computerised handling and exchange of information, data"[346].

The said initiative under the proposed regulation would have immense data protection implications for Union citizens. Currently, the ECDC has limited competencies to collect data and share it. A significant limitation observed during the Covid-19 outbreak was the lack of consistency and quality across data from the Member States as to what extent they wanted to share it[347]. This created significant limitations for the ECDC and other EU institutions to learn from real-time data, thereby limiting the ECDS's ability to take effective decisions to respond to the Covid-19 virus. The proposed system would abolish the current limitations. It would provide the Union with the competence to interchange data with all Member States of a personal nature such as electronic health records or lab results, and non-personal data to be used to respond and guide decisions in response to public health emergencies at the EU level[348].

Such an instrument could affect individual EU citizens' rights such as the right to privacy, specifically to data protection and would have to be balanced against the importance of protection of Union public health. In this respect, attention should be paid to informed consent enshrined in Article 9(2)(a) GDPR as the basis for the processing of health-related data. While in the Ebola outbreak in 2013-2016 the Member States had the "ultimate decision on how to comply with EU

[345] ibid.
[346] ibid.
[347] Alberto Alemanno, 'Towards a European Health Union: Time to Level Up' (2020) 11 European Journal of Risk Regulation 721 <https://doi.org/10.1017/err.2020.106> accessed 25 January 2021.
[348] European Commission Proposal for a Regulation of the European Parliament and the Council on serious cross-border threats to health and repealing Decision No 1082/2013/EU (n 13).

pandemic policies to adequately balance the right to informed consent and the protection of public health"[349], the proposed regulation would leave such decision in the hands of the Union.
The last observation should be made on the proposed regulation's suggested competence on the recognition of a public health emergency at the Union level, enshrined in Article 23 of the proposed regulation. Article 23 establishes that the Commission, based on ECDC's or any other relevant agency's opinion, would be granted the right and power to "formally recognise a public health emergency at the Union level"[350]. Such health emergencies may include pandemics and other health threats that affect public health at the EU level and thus strengthening the EU's response at a supranational level.

5.7 Conclusive Remarks

The examination of laws at the European level in Chapter 5 and the complex regulatory interplay between the laws allowed the research to establish the extent to which the use of big data, which includes personal data, is permitted in terms of the data protection legislation in healthcare and the limitations, if any, that can be drawn in terms of the processing of such data in emergencies. While the processing of personal, sensitive, and data concerning health is permitted under the GDPR, the processing of such data not only by governments of the Member States, but also by private organisations, requires checks and balances to be maintained in cases of emergencies, such as the Covid-19 crisis. Therefore, deploying digital health technologies for healthcare crisis management while ensuring that the balance of the personal fundamental freedoms against those of the society at large. In this regard, the chapter analysed the Covid-19 pandemic as healthcare emergency example and provided an in-depth analysis of the specific regulations and digital technology solutions implemented throughout the European continent to manage such emergency.
In this respect, a specific focus was placed on exposure notification applications, otherwise known in literature as contact-tracing application, as first-generation pandemic management technologies and on proofs of vaccination (specifically, the EU Green Certificate) as second-generation pandemic management technologies. Regarding the first technology deployed, it has been observed that in terms of data protection, contact-tracing technologies focus on the general principles of necessity, effectiveness, and proportionality, otherwise known as data-management principles. The proportionality concerning the exposure notification apps and geolocation apps entail that such apps should only be implemented to help respond to the pandemic through the modelling of the spread of

[349] KOLFSCHOOTEN (n 343).
[350] European Commission Proposal for a Regulation of the European Parliament and the Council on serious cross-border threats to health and repealing Decision No 1082/2013/EU (n 13).

the virus, and to notify individuals of their exposure to Covid-19, for instance, via exposure notification. The necessity principle, in terms of the GDPR, concerning exposure notification technologies, refers to the necessity for the performance of tasks considered to be in the public interest as enshrined in Article 6.1(e) of the GDPR. The adoption of contact-tracing technologies in the EU to contain and combat the epidemiological emergency of the Covid-19 in a highly complex context represented an unprecedented challenge for the Member States' governments. We observed that Europe's attempt to achieve the goal of managing the spread of Covid-19 was by incentivising the use of data, and through challenging the cultural and social fabric of the society, the way we communicate and interact with each other and our civic responsibility towards each other. Regarding proofs of vaccination, it was observed that a comprehensive regulatory regime and guidance was required for the introduction of proofs of vaccinations, not only in terms of data protection but considering ethical implications of such technologies. While the EU provided guidance on data protection issues, the ethical concerns were failed to be addressed to the full extent.

Also, we should note that technologies for the managing of public health crisis are neutral. They carry neither negative nor positive effects. Their deployment and effects are highly dependent on the jurisdiction such technologies are deployed in, and the social, cultural, and economical factors surrounding the society in that particular jurisdiction.

Finally, the chapter identified and addressed several shortcomings of the existing regulatory framework concerning healthcare emergencies at the Union level. The legislative proposal for the Regulation on Serious Cross-Border Threats to Health can be described as a building block for the Union's health crisis management as it would allow the Union to address new healthcare threats more rapidly at the EU level for a coordinated response. In this respect, the proposed regulation complements several already existing EU measures in the field of crisis management, including interoperability of health-related data through the EU Health Data Space, and by providing the infrastructure for such interoperability of data. It should be noted that the regulation provides the right and power to formally recognise a public health emergency. Such health emergencies may include pandemics and other health threats that affect health at the Union level.

The following chapter of the thesis deliberates and scrutinises several of the EU's legislative proposals and policy initiatives for big data and AI that will have an impact on the privacy and data protection of big data and AI-based digital health technologies. Therefore, the next chapter draws from the insight gained from the current legislative framework analysis and ponders how the new policy initiatives at the EU level were affected by the existing legislative framework and the extraordinary events of the recent years.

6 European Regulatory Initiatives: A Way Forward to Ensure the Right to Privacy and Data Protection in AI-Powered Digital Health Technologies?

The General Data Protection Regulation's implementation involved a "reimagination of geographical borders to match a new digital imaginary"[351]. With big data and Artificial Intelligence powering this new digital image, prospects for the digital health technology industry are bright. By 2030, the global market is set to double and reach 800 billion U.S. Dollars[352]. Similarly, the data economy is expected to reach 829 billion Euros by 2025[353]. Both markets are highly connected and concentrated, requiring innovative solutions for regulation, extended human capital, and skills. To stay ahead of this drastic expansion, the European Union strives to build a robust and competitive industry for big data- and AI-driven digital health technologies, based on European values.

As observed by researchers, the Union's attempts in this regard are based on the concept of digital sovereignty which are supplemented by the EU's interest in leading legislation in an interconnected world[354]. Still, it has been observed that the European Union lacks "control over digital technologies to ensure European values"[355], such as privacy and personal data protection. In this regard, an observation should be made that in the digital world, the GDPR is only a reactive legislation addressing breaches of personal data rather than actively addressing legislative fragmentation, which is visible from data infringement scandals, such as Cambridge Analytica[356]. Nevertheless, policy initiatives such as the European Health Data Space, the EU Digital Decade 2030, and the EU Commission's proposal for the regulation of Artificial Intelligence, dubbed the AI Act, are expected to pave the way forward for the legislation of the digital world, including the digital health technology sector, rather than play a secondary, catch-up role.

From a legislative standpoint, governments and entities that adopt big data and AI-based technologies in the healthcare sector will need to establish proactive and durable policies to protect

---

[351] Brett Aho and Roberta Duffield, 'Beyond Surveillance Capitalism: Privacy, Regulation and Big data in Europe and China' (2020) 49 https://doi-org.proxy.bnl.lu/10.1080/03085147.2019.1690275 187 <https://www-tandfonline-com.proxy.bnl.lu/doi/abs/10.1080/03085147.2019.1690275> accessed 14 December 2021.

[352] 'Medical Devices 2030 - KPMG' (18 January 2021) <https://home.kpmg/it/it/home/insights/2018/01/medical-devices-2030.html> accessed 26 October 2021.

[353] 'The European Data Strategy' <https://ec.europa.eu/commission/presscorner/detail/en/fs_20_283> accessed 20 February 2020.

[354] Luciano Floridi and others, 'Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies' [2021] Internet Policy Review:Journal on Internet Regulation 1 <https://policyreview.info/articles/analysis/safeguarding-european-values-digital-sovereignty-analysis-statements-and-policies>.

[355] ibid.

[356] Aho and Duffield (n 352).

individuals[357]. Some academics claim that such policies should focus on three priority areas for policies: access and benefit sharing, accountability and transparency, and quality and safety[358].

Great focus is placed on personal and group privacy, both in IoT and digital health contexts. In the digital health context particularly, privacy covers topics such as confidentiality and personal data protection, while on a broader scale, such as health IoT, the "challenges concern the realignment of traditional matters of privacy and data protection brought on by structural data sharing and new levels and layers of connectivity and communication, (or) collective, rather than individual, data"[359,360].

Research also addresses concerns as to what extent big data processing is compatible with the primary rules and principles of the GDPR such as purpose limitation and data minimisation[361]. What is more, in recent years the research tends to focus on, for example, the complex relationship between the phenomena of big data, Artificial Intelligence, and Article 22 of the GDPR[362]. Nevertheless, questions relating to the balancing of the right to health driven by digital health technologies with the right to privacy and data protection remain secondary in academic discussion. This chapter therefore analyses and attempts to engage in a discussion on whether the current European regulatory initiatives can pave the way forward to reconciling these two fundamental rights in a new digital imaginary.

Considering the above premises and the future of digital health technology sector, this chapter is construed as follows. The chapter starts with a reflection and deliberation of key policy initiatives such as the European Health Union and the Digital Decade 2030. Then, the EU Data Strategy and the proposal for the Creation of the Common Health Data Spaces are examined against the right to data privacy, data protection, and the right to health. The chapter then moves on from the discussion of European policy initiatives that affect the digital health technology landscape to the analysis and discussion of the EU's regulatory initiatives, namely the proposal for the EU Artificial Intelligence Act. In this regard, the chapter provides an analysis of the current draft of the proposal and its impact on the balancing of privacy, data protection, and health in the digital health technologies environment. This part of the chapter also provides a noteworthy interconnection of the EU AI Act proposal considering the existing Medical Devices Regulation, arguably the main piece of

[357] Effy Vayena and others, 'Policy Implications of Big Data in the Health Sector.' (2018) 96 Bulletin of the World Health Organization 66 <http://www.ncbi.nlm.nih.gov/pubmed/29403102> accessed 27 November 2019.
[358] ibid.
[359] ibid.
[360] Ugo Pagallo, Massimo Durante and Shara Monteleone, 'What Is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT' 59.
[361] Pagallo, 'The Legal Challenges of Big data: Putting Secondary Rules First in the Field of EU Data Protection' (n 151).
[362] Monica Palmirani, 'Big Data and Knowledge' (2020) IX Rivista di filosofia del diritto 73 <https://www.rivisteweb.it/doi/10.4477/97021> accessed 10 December 2021.

legislation in the digital health innovation sector in the European Union. Finally, the chapter concludes with several observations on the impact of the discussed policy and regulatory initiatives to the digital health technology sector and how the new initiatives have reshaped the EU legislator's view on the future of digital healthcare regulations, AI, big data, data protection, and privacy.

6.1 An Excursus on the European Health Union and on the EU Digital Decade 2030

Built on the EU's Digital Strategy, the EU's Digital Decade Strategy is a guiding compass for the European Union to become a digital force by 2030. It is a compass that sets ambitious targets for the digitalisation of different aspects of the EU infrastructures and areas. Interestingly, the said strategy pays great attention to strengthening Europe's "digital sovereignty", a term that often appears in EU documents regarding the regulation of the digital world, yet as observed by some academics, lacking a common understanding[363]. The means of strengthening Europe's so-called digital sovereignty include, inter alia, the digitalisation of the healthcare services within the EU, from promoting digitally enabled solutions for healthcare, mHealth, telehealth, to ensuring secure and performing sustainable digital infrastructures for such digital healthcare solutions. Still, such digitalisation is not possible without the driver of digitalisation, big data. In fact, the Europe's Digital Decade communication addresses the vast volume and variety of data processed, thus addressing big data. In this regard, the Digital Decade strategy acknowledges that current European solutions for the processing and protection of big data are not sufficient, and that Europe should focus on future state-of-the-art, such as edge computing and quantum computing, with a specific example of the digital twins[364]. It is clear from the Digital Decade Strategy that healthcare is one of the areas in the EU that will feel digitalisation the most. In fact, it could be argued that the ongoing Covid-19 crisis exposed the lack of digitalisation which, to some extent, may impede the EU's recovery from Covid-19, as observed by the same Digital Decade Strategy. The digital transformation of the EU is led by digital principles and digital rights, proclaimed by the European Commission in January 2022. The proclaimed digital rights include people at the centre of the digital transformation, a call to support solidarity and inclusion, to ensure freedom and choice online, foster participation in digital public space, increase safety and security of individuals, and promote sustainability in the digital future. The digital health sector will particularly focus on inclusion and provision of health services to all EU citizens and on safety and security of individuals in the digital transformation of healthcare services. Arguably, the focus rests not only

[363] Floridi and others, 'Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies' (n 355).
[364] 'Europe's Digital Decade: Digitally Empowered Europe by 2030' <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983> accessed 16 March 2021.

protecting individuals from harmful healthcare services, but also from cybercrime, including data breaches and cyberattacks.

In this respect, the EU's initiative on the European Health Union will be discussed and a few observations will be made on the proposal for the European Health Union. To start with, civil society and academia had discussed, and it is widely acknowledged that the Union's limited competences in the healthcare sector had delayed the EU's response to the ongoing Covid-19 healthcare crisis. Such a delay varied from late initial response at the beginning of pandemic to, for example, an authorisation of the Covid-19 vaccines, as acknowledged by the President of the European Commission herself[365].

The announcement on the building of the European Health Union, on 25th October 2020 by the European Commission can be argued to be a response to the shortcomings of Covid-19 pandemic management. Some may call it a necessary political move in times of crises to insinuate actions to ensure stability on the European continent, following the Covid-19 pandemic.

While the initiative's name seems all encompassing, the core objective of the European Health Union is to expand the currently limited ECDC's powers in cases of EU-wide healthcare crises by establishing an EU-wide health crisis response mechanism. This is due to the fact that the European Union's ECDC has limited competences in the field of health and healthcare crises, due to Article 168 TFEU. While the European Treaties have left health systems out of the scope of harmonisation, it does not prohibit closer integration, which became the basis of the creation of the EU Health Union.

It is claimed that such a health crisis management mechanism would allow the Union to respond to health crises faster, ensure that medical supplies are available, and guarantee that Member States work together to improve prevention, treatment, and aftercare of diseases[366]. The aims of such EU's Health Union are clear: they focus on the protection of the health of EU citizens, improving resilience of Member States' health systems to crises, and pandemic prevention.

The Covid-19 crisis is the driving force of the Commission's attempts to form a European Health Union able to face various healthcare crises. Thus, the proposed Health Union's actions focus almost exclusively on public healthcare crises and their management. For instance, in the previous chapter we analysed the EU's response to Covid-19 management through the proposal for a regulation on the Serious Cross-Border Threats to Health, which forms part of the EU's Health Union action plan.

---

[365] 'Covid: EU's von Der Leyen Admits Vaccine Rollout Failures - BBC News' <https://www.bbc.com/news/world-europe-56009251> accessed 13 December 2021.

[366] Beaussier and Cabane (n 341).

Other announced key initiatives also focus on public health crisis response mechanisms, such as public health crisis preparedness and response mechanisms. Specifically, the launch of a new "European Health Emergency Preparedness and Response Authority"[367] (hereafter, HERA), which is tasked to develop, produce, and procure medical countermeasures before and during a public health crisis. Even the EU's pharmaceutical strategy, part of the EU's Health Union action plan, focuses highly on enhancing resilience and crisis preparedness through diversified supply chains and environmental sustainability. While other initiatives, such as cancer research and treatment, also form part of the Health Union's action plan, these appear to take a secondary role in the establishment of the European Health Union.

Still, a question remains: should the European Union go further than the current packaged plan for the building of the EU Health Union? Differences between national health systems remain at the core of this debate and are particularly apparent in times of crises where national governments are directly exposed if they fail to protect the lives of their citizens. During the Covid-19 pandemic, for example, the Member States, equipped with the harmonised tool of the EU digital Covid vaccination certificate, have continued to deviate from ECDC and the EU advice on epidemiological criteria, to stick to national health requirements for travellers.

The joint vaccine purchase strategy at the EU level, can thus be considered an exceptional solidarity decision taken in the context of global race for vaccine-nationalism. In this regard, the European Health Union has proposed some new ideas that would allow the European approach to crises management to be streamlined. Still, rather than establishing a true health union which, for instance also focuses on facilitating equal health standards between the Member States, it establishes an integrated European health crises governance system model with integrated minimum requirements for preparedness, prevention and response to health crises, minimum standards of resilience for health systems, and joint responses in common-interest areas such as travel and transport, and exchange of health information. The Covid-19 context can thus be regarded as a "favourable contextual condition"[368] for the establishment of such health crises governance system. Consequently, it can be observed that the "envisaged European Health Union won't entail a Copernican revolution"[369] as the outcome of the Covid-19 pandemic. Lastly, it should also be added that the European Health Union comes as a politically planned response to manage public's disappointment regarding the Union's incapacity to respond to the Covid-19 pandemic, even with the crisis management mechanisms that were available.

---

[367] 'Building a European Health Union' <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2041> accessed 7 December 2020.

[368] Giulia Bazzan, 'Exploring Integration Trajectories for a European Health Union' (2020) 11 European Journal of Risk Regulation 736.

[369] Alemanno (n 348).

6.2 The European Data Strategy: on the Proposal for the Creation of the European Health Data Space

Data has been the "key asset for the economy and our societies similar to the classic categories of human and financial resources"[370] for the past few decades. The European Union has recognised that the digital transformation over the next five years will be crucial to put the Union on the map as a competitive jurisdiction and a market for new technologies' development[371]. The European Strategy for Data, announced in early February 2020, forms one of the first pillars of the new digital strategy of the European Commission. It aims at creating a single European data market through the establishment of the European Data Spaces. Such EU Data Spaces would facilitate the availability of data for use and reuse, without individuals who generate the data being left without control over their personal data[372]. In this respect, the strategy establishes that European values, such as the right to privacy and the rights to personal data protection, are to be guaranteed in the common data spaces. In fact, the European Data Strategy emphasises that privacy and particularly data protection should be fully respected in the reach of the goal of the common data spaces[373].

Nonetheless, we should also note that some authors argue that one of the GDPR's objectives is to promote the free flow of data within the internal market and appear to reflect aspects of economic regulations, which would facilitate the creation of a health data market, therefore the framework "disavows fundamental rights protection objectives to promote research based on health data and related market objectives"[374,375]. This is however a short-sighted view. The GDPR, since its inception, was drafted and to date remains a regulation to ensure fundamental rights to data protection, notwithstanding the EU's established market objectives. In fact, the GDPR neither facilitates nor promotes any market objectives as the scope of the GDPR is applicable throughout all markets in the EU where personal data is processed. Thus, it focuses on the promotion of the fundamental right to data protection throughout the European Union.

Considering the above, the healthcare sector is recognised by the Commission as one of the nine strategic sectors where the pooling of technological resources and sharing of data would not only

[370] Svetlana Klessova and others, 'ICT Policy, Research, and Innovation: Perspectives and Prospects for EU-US Collaboration' [2020] ICT Policy, Research, and Innovation: Perspectives and Prospects for EU-US Collaboration 1 <https://onlinelibrary.wiley.com/doi/book/10.1002/9781119632481> accessed 2 August 2022.

[371] 'European Data Strategy | European Commission' <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en#documents> accessed 1 July 2020.

[372] 'A European Strategy for Data'.

[373] 'European Data Strategy | European Commission' (n 372).

[374] Klessova and others (n 371).

[375] Giulia Schneider, 'Health Data Pools under European Policy and Data Protection Law: Research as a New Efficiency Defence?' (2020) <https://www.rand.org/pubs/> accessed 7 January 2021.

improve the quality of access to healthcare, but also support scientific research and allow authorities to take evidence-based policy decisions.

The EU's powers regarding the healthcare sector remain limited by the EU Treaties. Particularly, Article 168 TFEU which provides the EU with the powers to act in public health. The drafting of the article outlines that the goal of common EU policy on health is limited to the population-level measures and away from any actions to be taken in the healthcare services area. In this regard, we should note that there are only few areas where binding legislation is called for, such as "concerns of the quality and safety standards for substances of human origin, blood and blood derivatives"[376], the setting of high standards for medicinal products and devices, and measures in the veterinary and phytosanitary fields[377].

Furthermore, instruments provided by Article 168 TFEU include the provision of financial support by the EU and the power for the Council of Ministers to adopt recommendations in support of the said article. In addition, Article 168 TFEU provides for the Member States to coordinate their health policies. Since EU level action in health is limited to population-level measures, it is no surprise that one of the areas where the EU action on health has been coordinated consistently is disease control and other cross-border threats to health. Coordination of measures in cross-border disease and the health threat area began in the early 1980s when the EU commenced funding research, training, and disease-specific monitoring networks[378].

Nonetheless, the European Data Strategy claims that the establishment of "a common European Health Data Space is essential for advances in preventing, detecting, and curing diseases as well as for informed, evidence-based decisions to improve the accessibility, effectiveness, and sustainability of the healthcare"[379] systems. Such an EU Health Data Space would have the potential to improve "evidence-based decisions to improve the accessibility, effectiveness, and sustainability of the healthcare systems, support the work of regulatory bodies in the healthcare system, the assessment of medical products and demonstration of their safety"[380] and efficacy.

Even further, one of its aims is to facilitate citizens access and control of their personal data, yet we should observe that the data strategy and the actual proposal for the regulation of the EU Health

---

[376] Greer SL, Fahy N and Rozenblum S, 'EU Action for Health - Everything You Always Wanted to Know about European Union Health Policies but Were Afraid to Ask' (2019) 3 European Observatory on Health Systems and Policies <https://www.ncbi.nlm.nih.gov/books/NBK551073/> accessed 2 August 2022.

[377] European Commission, Regulation (EU) 2021/2282 of the European Parliament and of the Council of 15 December 2021 on health technology assessment and amending Directive 2011/24/EU (Text with EEA relevance) PE/80/2021/INIT 2021 1.

[378] 'EU Action for Health - Everything You Always Wanted to Know about European Union Health Policies but Were Afraid to Ask - NCBI Bookshelf' <https://www.ncbi.nlm.nih.gov/books/NBK551073/> accessed 1 July 2020.

[379] The Council, The European Economic and Social Committee and the Committee of the Regions 'A European Strategy for Data' <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066> accessed 9 September 2020.

[380] 'A European Strategy for Data' (n 373).

Data Spaces both fail to address how this would be implemented in practie. Indeed, the EDPS-EDPB joint opinion published in July 2022, also addressed similar shortcomings, extending its view that the proposal "may even weaken the protection of the rights to privacy and to data protection, especially considering the categories of personal rights of data subjects already provided for in the GDPR"[381].

Interestingly, the data strategy claims that the GDPR has "created a level playing field for the use of health personal data, fragmentation remains within and between Member States and the governance models for accessing data are diverse"[382]. The strategy further notes that such fragmentation could be addressed by a complementing horizontal framework for health data[383]. Again, the Commission here failed to address what horizontal frameworks it intends to establish for health data.

What is more, in the context of big data and digital health technologies, the EU Health Data Space initiative specifically mentions the term big data. It references the term as one of the aims of the EU Health Data Space, i.e., supporting big data (in health) projects promoted by the network of regulators[384]. This would eventually lead to advanced regulatory initiatives by the Member States in public health, as well as facilitating research, diagnosis, and innovation in the healthcare sector.

The establishment of such an EU Health Data Space, which includes a vast variety of actors, brings about several data protection-related concerns. Such concerns include the collection, processing, use, reuse, and transfer of both personal and personal sensitive data in terms of the GDPR. Thus, it will require the EU Health Data Space's conformation with the GDPR's established principles and norms.

Indeed, the EDPS was quick to pick up on the European Commission's intents to establish the European Health Data Space. In its opinion on the EU's Data Strategy, the EDPS has underlined that any creation of such common space will have a "significant impact on the processing of various health related personal and personal sensitive health data"[385].

From the analysis of the text on the creation of the European Health Data Space and the EDPS opinion on it, privacy and data protection related concerns can be grouped into the following categories:

1. Processing of personal and non-personal health data;
2. Ethics of processing personal and non-personal health data;

---

[381] EDPB, 'EDPB-EDPS Joint Opinion 03 / 2022 on the Proposal for a Regulation on the European Health Data Space Adopted on 12 July 2022' 1 <https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en>.

[382] 'European Data Strategy | European Commission' (n 372).

[383] 'A European Strategy for Data' (n 373).

[384] ibid.

[385] 'Preliminary Opinion 8/2020 on the European Health Data Space | European Data Protection Supervisor' <https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-82020-european-health-data-space_en> accessed 30 November 2020.

3. Data governance mechanism for the EU Health Data Space.

To start with, in its opinion, the EDPS underlined that to create a common European Health Data Space a "robust and harmonised legal regime would need to be established applicable specifically to health data, a regime that further harmonises data protection rules across the board"[386]. This is a thought-provoking elaboration by the EDPS. Currently, personal health data, i.e., data related to health in the language of the GDPR, is protected and regulated exclusively under the GDPR. Nonetheless, it seems that we may expect an establishment of a sectorial legislation within the general framework of the GDPR for health data, in the context of EU Health Data Space that would further extend the limits of data protection. Additionally, the EDPS further noted that codes of conduct for sharing health data may serve as an effective enabler for the cross-border exchange of such data in the EU[387].

Furthermore, as already observed in Chapter 4, the distinction between personal health-related data and non-personal health-related data is not straightforward. With regards to the creation of the EU Health Data Space, the EDPS also observed a similar aspect. The EDPS noted that the EU Data Strategy makes "a distinction between three categories of data, namely non-personal, personal and mixed data sets"[388]. Mixed data sets may, in practice, infer or generate personal data in terms of the GDPR. This observation serves as a caution to the drafters of the strategy to reconsider the somewhat strict (or rather, unrealistic) division between personal and non-personal health data in the strategy[389].

A few observations should be made regarding the legal basis for the processing of personal data and special categories of data. It can be noted that to protect personal data, the EU Health Data Space must process health data in line with the main data protection principles: legality, transparency, necessity, proportionality, integrity, and confidentiality.

Also, with respect to the processing of personal data, Article 6 of GDPR provides a lawful legal basis for such processing. The legal basis under Article 6 includes consent (art. 6(1)(a)), processing necessary to protect the vital interest of the data subject or other natural person (art. 6(1)(d)), processing necessary for the performance of a task carried out in the public interest (I. 6(1)(e)), which all appear to be the applicable legal basis for the lawful processing of personal data in the envisaged European Health Data Space. The EDPS, however, noted that it considers Iicle 6(1)(e) as the most appropriate legal basis for the processing of personal data, arguing that the processing of

[386] EDPS, 'Opinion 3 / 2020 on the European Strategy for Data' (2020) <https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf>.

[387] Supervisor (n 135).

[388] ibid.

[389] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.) 2018 (OJ L 303, 28112018, p 59–68 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)).

personal data will "serve the public interest and the processing should be done in the exercise of official authority vested in the controller"[390].

Also, considering that the EU Health Data Space would be processing health-related personal data, such data would fall under the special categories of data under Article 9 of the GDPR. Thus, additional safeguards to the processing of such data under Article 9 would need to be satisfied. Article 9(2) of GDPR provides several exemptions when processing of special categories of data is permitted[391], all of which could be the legal basis for the processing of health-related personal data in the EU Health Data Space. Yet, the EDPS considers only Articles 9(2)(i) and 9(2)(j) of the GDPR, which refer to the processing necessary for reasons of public interest in health and "for archiving purposes in the public interest, scientific or historical research purposes or statistical purpose, as the main basis for the processing of health-related data"[392] for the EU Health Data Space. Considering that the European EU Health Data Space aims to include different actors in the access and use of such data, the exemptions provided by the EDPS appear to contradict the main goal of the common data spaces, that is, the access and use of data.

Also, the EU Health Data Space is expected to involve the participation of several key actors, such as DPAs, individuals, research institutes, private bodies and so on. Nonetheless, it is not yet clear what their role would be going forward in the processing of such data. In this respect, the EDPS required the Commission not only to clarify the types of data that will be made available, but also the precise "roles and responsibilities of the parties involved, as regards to the identification of controllers withing the EU Health Data Space"[393]. Thus, it can be observed that data protection principles should be integrated and be positioned at the heart of the EU Health Data Space to protect the fundamental rights and freedoms.

Likewise, ethics of data[394] and its framework in the EU Health Data Space also take a prominent role. In this respect, we emphasise that attention should be paid to the ethical use of data within the EU Health Data Space. It is therefore suggested that ethical committees within the Member States are established and consulted to ensure the ethical management, use and processing of personal and personal sensitive data in this framework. A noteworthy aspect here, however, is the EDPS consideration that ethical issues are mainly related to the lawful further processing of data such as "those relating to personal objections to certain private sector stakeholders having access to the

---

[390] 'Preliminary Opinion 8/2020 on the European Health Data Space | European Data Protection Supervisor' (n 386).
[391] More in depth information on legal basis can be found in Chapter 4 of the thesis.
[392] 'Preliminary Opinion 8/2020 on the European Health Data Space | European Data Protection Supervisor' (n 386).
[393] ibid.
[394] Floridi L and Taddeo M, 'What Is Data Ethics?' (2016) 374 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20160360 https://royalsocietypublishing.org/doi/10.1098/rsta.2016.0360, accessed 10 June, 2021.

individual's sensitive personal data"[395]. Such an EDPS concern also clarifies why the EDPS would only consider Articles 9(2)(i) and 9(2)(j) as legal grounds for processing personal sensitive data as the EDPS has long pushed to limit access for private actors to personal data.

Following the publication of the EU Data Strategy, on 3rd May 2022 the Commission also published a proposal for a regulation on the establishment of the common European Health Data Space[396]. The proposal's scope is limited to the establishment of "common standards and practices, infrastructures, and a governance framework for the primary and secondary use of electronic health data"[397], as enshrined in Article 1 of the proposal. The proposal applies not only to the manufacturers, suppliers of electronic health record systems, and wellness applications which are placed on the EU market, but also to controllers and processors within the EU, and data users to whom electronic health records (hereafter, the "EHRs") are made available by data holders in the Union (Article 2 of the proposal)[398].

In essence, the proposal establishes various interoperability mechanisms for the sharing of EHRs collected from various medical, mHealth, and telehealth devices, hospitals, and other healthcare entities, for both primary and secondary use (e.g., research). It also establishes grounds for access to such electronic health record data (e.g., Article 4 which establishes access to data by health professionals), the rights of the data holders to access their electronic health records (Article 3), electronic health record exchange format (Article 6), identification management (Article 9), cross-border infrastructure for the primary use of EHR (Article 12) and so on. Interestingly, the proposal also establishes EU-wide conformity specifications for EHR systems (Article 23) and the requirement for the EHRs to have the conformity declaration (Article 26), together with a CE marking (Article 27). With respect to the secondary use of data, Article 33 establishes the minimum categories of electronic data that data holders shall make available for secondary use. These categories include electronic data such as EHRs, human genetic and genomic data, pathogen genomic data, and "data impacting on health, including social, environmental behavioural determinants of health"[399]. Article 34 further establishes an exhaustive list of purposes for access to such secondary data which has the "the intended purpose of processing" pursued in accordance with the established purposes in Article 34. While the list of such processing purposes is limited, the drafting of the text leaves space for interpretation as to what is the "intended purpose" and who will decide (likely, national competent authorities) whether the "intended purpose" is in line with the

[395] 'Preliminary Opinion 8/2020 on the European Health Data Space | European Data Protection Supervisor' (n 386).
[396] Full name of the proposal: Proposal for a regulation of the European Parliament and of the Council on the European Health Data Space. Accessible at: https://eur-lex.europa.eu/legal content/EN/TXT/?uri=CELEX%3A52022PC0197
[397] European Commission Proposal for a Regulation on the European Health Data Space (Text with EEA relevance) (n 16).
[398] ibid.
[399] ibid.

processing activities defined in the said Article 34. For example, imagine a situation where the "intended purpose" of the processing is related to the provision of personalised healthcare (Article 34(h)). A situation could arise where private organisations would likely be able to use this exemption to access personal sensitive data, which would allow them to develop personalised mHealth or telehealth technologies, which would, in the end, economically benefit private entities at the expense of individual personal sensitive data. While the benefit to an individual who would invest in such a personalised digital health device could be significant (again, it would highly depend on the technology developed, but consider instances where organisations could use the above exemption to access personal sensitive data to develop wellness tools such as personalised dietary plans, whose benefits have not been proved by research) it nonetheless poses ethical questions as to who will receive actual benefits from the sharing of data: the user or a private entity.

Besides, the proposal moves away from ensuring that the data subject's rights enshrined in the GDPR will remain at the core when considering the EU Health Data Spaces. In recent years we have observed movements to bring control over one's data back to the data subjects. However, the EU Health Data Spaces proposal seems to steer away from this. This is due to the lack of the transposition of the data subject's rights into the said proposal and its effects on such rights. For example, it is not clear how the data subject's rights, such as the right to explanation will be ensured in the proposal. Likewise, data subject's rights such as the right to be forgotten, enshrined in the GDPR should be further explored.

Notwithstanding issues that ought to be clarified from a data protection point of view, the EHDS proposal may be the necessary tool that would facilitate HERA's and the ECDC's rights in the pandemic and public health crisis observation and prediction. This is due to the fact that the creation of an interoperable Health Data Space at the European level would address the lack of epidemiological data, that was also observed by the EU during the Covid-19 crisis. Facilitation of monitoring, surveillance, and research of the 'unknown' public health crisis is after all a core competence of HERA and the ECDC for these two agencies to be able to timely respond to future health crisis.

Balancing fundamental rights to privacy, data protection, and improved health will remain a battle in the European Commission's proposal for the EU Health Data Space. Even if the right to privacy and data protection are not absolute rights and may be limited, any such limitations would however require a careful analysis. Therefore, detailed data access restriction policies and evaluations on case-by-case basis will take a primary role as governance mechanisms to ensure legal access and processing of personal data, in line with the GDPR. The EDPS has also acknowledged that the governance of the EU Health Data Space and of data governance itself will be paramount to the

success of the project[400]. Such mechanisms would have to be capable of assuring a lawful, transparent, and ethical management of the data involved, including effective accountability mechanisms in the EU Health Data Space. The governance framework of the EU Health Data Space should include at least the main actors, so far identified as entities making data available to the data space, the users of the data spaces, the Member States' contact points, and the DPAs. Additionally, the governance framework should also ensure the compliance with Schrems II decision and the EU values of data protection and privacy. Finally, considering the EU's initiative on creating an EU Health Data Space, one is to reflect that such a space may become an instrument allowing for better readiness of future health related crises.

6.3 From Big data Powered Digital Health Technologies to AI-Powered Digital Health Technologies: Implications of the Proposal for the Regulation of Artificial Intelligence

Steering away from European policy initiatives in the digital sector and digital health technology sector, this section of the chapter focuses on the EU Commission's regulatory initiatives for the digital, the so-called EU Commission's proposal for the regulation of Artificial Intelligence (dubbed the "AI Act proposal") and its impact on the balancing of privacy, data protection and the right to health in digital health technologies.

In this regard, this segment is structured as follows. We firstly briefly outline the background of the AI Act proposal. Then, an overview of the ethical and legal criticism of the proposed AI Act in relation to data protection, privacy, and health in the existing legal framework is provided. The following section then presents an in-depth analysis of the proposed AI Act's impact on digital health technologies, focusing on high-risk AI systems. After this, the subsequent section critically analyses the provisions of AI Act in the broader context of digital health technologies by examining the interplay between the Medical Device Regulation and the AI Act proposal. This segment of the chapter finishes with remarks on whether the current proposal and the EU policy initiatives are enough to establish a clear set of rules applicable to AI-powered digital health technologies.

6.3.1 Background on the AI Act Proposal

Evolving from simple statistical observations on big data implemented in digital health technologies, the healthcare industry is moving forward to implement more complex digital health technologies using Artificial Intelligence. AI systems have the potential to "support socially and environmentally beneficial outcomes and provide critical competitive advantages to European

[400] 'Preliminary Opinion 8/2020 on the European Health Data Space | European Data Protection Supervisor' (n 386).

companies and economies, improve efficiency and consistency in decision-making processes and enable new solutions to complex problems"[401,402].

The promising benefits of AI in digital health sector include a provision of more equitable health, more patient-centric treatments, use of wearable AI technologies, advanced disease prevention, and streamlined healthcare providers' internal processes. In other words, it can be summed up that the main benefits of AI in healthcare do not differ from those in other fields and include cost reduction, saved time (time efficiency), and increased staff availability.

Considering the many benefits of AI, the European Union has attempted to position itself as a "'leader by example for the good governance of AI"[403] in digital health technologies to become a competitive global market[404]. It can be observed that the EU has learnt its lessons from allowing big-tech companies to use a "build first, ask for forgiveness later" approach in highly innovative, data-based markets with European citizens feeling consequences of such risks, such as can be observed from data leaks such as the Cambridge Analytica scandal.

The discussion on whether artificial intelligence should be regulated or not has been highly debated in scientific literature. For instance, an AI regulatory framework was proposed in 2015 by Scherer[405], focusing on the United States. The recent initiative by the Council of Europe's Ad hoc Committee on Artificial Intelligence (hereinafter, "CAHAI") has recommended a legally binding treaty on Artificial Intelligence that would protect, inter alia, democracy, human rights, and the rule of law[406].

Still, few tangible examples of attempts to regulate AI and related implications to society at large have been adopted. In Europe, Member States such as Malta have implemented voluntary AI assurance mechanisms, in essence, requiring certain AI systems to undergo a so called "AI system audit"[407]. Consequently, to avoid diversified regulatory approaches, in 2021 the European

---

[401] Luciano Floridi and others, 'Conformity Assessments and Post-Market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation' [2021] Minds and Machines 1 <https://link.springer.com/article/10.1007/s11023-021-09577-4> accessed 14 December 2021.

[402] Mariarosaria Taddeo and Luciano Floridi, 'How AI Can Be a Force for Good' (2018) 361 Science 751 <https://www.science.org/doi/abs/10.1126/science.aat5991> accessed 14 December 2021.

[403] Luciano Floridi, 'The European Legislation on AI: A Brief Analysis of Its Philosophical Approach' (2021) 34 Philosophy & Technology 215 <https://link.springer.com/10.1007/s13347-021-00460-9> accessed 23 June 2021.

[404] EU Commission, Proposal for a Regulation of the European Parliament and of the Council laying dow harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts COM/2021/206 final 2021.

[405] Matthew U Scherer, 'Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies' (2015) 29 Harvard Journal of Law & Technology <https://heinonline.org/HOL/Page?handle=hein.journals/hjlt29&id=365&div=15&collection=journals> accessed 20 December 2021.

[406] 'AI: Decoded: The World's First AI Treaty — Timnit Gebru's New Gig — The European Parliament Starts Work on the AI Act – POLITICO' <https://www.politico.eu/newsletter/ai-decoded/the-worlds-first-ai-treaty-timnit-gebrus-new-gig-the-european-parliament-starts-work-on-the-ai-act-2/> accessed 20 December 2021.

[407] Joshua Ellul and others, 'A Pragmatic Approach to Regulating Artificial Intelligence: A Technology Regulator's Perspective' <http://arxiv.org/abs/2105.06267> accessed 20 December 2021.

Commission announced a proposal for the regulation of Artificial Intelligence, otherwise known as the "AI Act"[408,409]. The European proposal for the AI Act unifies the European approach to regulating Artificial Intelligence and can be considered a bold move in this respect.

The proposal for AI Act is a horizontal approach to regulation, is not sector-specific but aims at laying down general rules for the use of Artificial Intelligence. It is harmonised with sector-specific EU legislation as far as it is mentioned in the proposal itself. The Commission therefore hopes that such a horizontal approach will ensure future-proof AI legislation that is flexible enough when considering technology advancements.

The legal basis for the AI Act proposal lies in Articles 114 and 16 TFEU. The latter is only the basis insofar as it contains specific rules on the protection of individuals regarding personal data processing. In this regard, it can be observed that under Article 16 TFEU, the AI Act proposal needs to ensure independent oversight for compliance regarding the processing of personal data which is also required under Article 8 of the EU CFHR.

Article 114 TFEU, on the other hand, has been chosen as the legal basis for the regulation due to the necessity to prevent the fragmentation of the internal market that arose from the explosion of voluntary national legislative attempts towards AI, including international technical standards that would create obstacles to cross-border movement of AI. In this respect, it is important to note that the proposed rules in the AI Act would apply directly to both public and private bodies within the EU and outside, as long as an AI system is placed on the European market[410] or its use affects EU citizens as observed in Article 2(1) of the proposed AI Act, leading to the so-called "Brussel's effect".

The proposal includes an attempt to define AI. According to the proposal, an "AI system is defined as a software, which is developed with machine learning, logic- and knowledge-based or statistical approaches" and which can "generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with" based on set "human-defined objectives"[411] (Art. 3(1), Annex I of the AI Act proposal). While it is not in the scope of the thesis to define artificial intelligence for regulatory purposes, it is nonetheless important to mention that precisely the definition of the AI in the proposal provides the scope of the limits of the regulation.

---

[408] EU Commission Proposal for a Regulation of the European Parliament and of the Council laying dow harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts COM/2021/206 final (n 405).

[409] The European Commission, Annexes to the Proposal for a Regulation of the European Parliament and of the Council Laying down harmonised rules on Artificial Intelligence (Artificial INtelligence Act) and amending certain union legislative acts 2021.

[410] ibid.

[411] 'The GDPR and the Artificial Intelligence Regulation – It Takes Two to Tango? - CITIP Blog' <https://www.law.kuleuven.be/citip/blog/the-gdpr-and-the-artificial-intelligence-regulation-it-takes-two-to-tango/> accessed 2 August 2022.

Furthermore, the proposal for the AI Act is a risk-based regulation. In particular, the proposal classifies AI systems into minimal, limited, high, and unacceptable risk AI systems. Low and minimal risk AI systems have minimal compliance requirements, such as transparency obligations regards communication as enshrined in Article 52 (consider, for example, chatbots). Great focus is placed on compliance of high-risk AI systems. Unacceptable risk AI systems are banned straightaway. As defined in Article 5 of the proposal, unacceptable risk AI systems include social scoring by governments, exploitation of vulnerabilities of specific groups of persons such as children, the use of subliminal techniques, or real-time remote biometric identification systems in publicly accessible spaces used for law enforcement and so on[412].

Regarding high-risk AI systems, the AI proposal establishes that such systems are required to comply with certain rules both pre-market and post-market, which are based on the idea of co-regulation through standardisation and certification[413]. Such co-regulation through common standardisation is a major innovation, as compliance with the requirement would have to be done ex ante, through a conformity assessment to establish that high-risk AI systems, in accordance with the regulation[414]. Furthermore, another key innovation is a mandate for an ongoing post-market monitoring system to detect problems in use and to mitigate them.

Lastly, the proposal expands beyond the regulatory compliance of AI systems. It also introduces the creation of a European Artificial Intelligence Board (hereafter, the "EAIB") that would facilitate the development of AI standards and introduce regulatory sandboxes, and voluntary codes of conduct for certain AI systems. Besides the creation of the EAIB, the proposal also establishes fines up to 6% of annual worldwide turnover for breaching the rules on high-risk systems. All other breaches would be subject to fines of up to 4% of annual worldwide turnover.

6.3.2 The Criticism and the Appraisal

The proposed AI Act has received both criticism and appraisal. On the one hand, the AI Act could be considered to place the European Union in a position of "leadership by example" for the good governance of AI technologies, especially when interacting with competing jurisdictions, such as China or the U.S., in the field[415]. At the same time, the proposal is said to provide the "much-needed infrastructure surrounding AI as technology through the certification mechanism of specific

[412] The European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts 2021.

[413] Martin Ebers, 'Standardizing AI - The Case of the European Commission's Proposal for an Artificial Intelligence Act' [2021] SSRN Electronic Journal <https://papers.ssrn.com/abstract=3900378> accessed 20 December 2021.

[414] The European Commission Annexes to the Proposal for a Regulation of the European Parliament and of the Council Laying down harmonised rules on Artificial Intelligence (Artificial INtelligence Act) and amending certain union legislative acts (n 410).

[415] Floridi (n 404).

AI systems with EU values and ethics embedded at regulatory and certification levels"[416]. Furthermore, the risk-based approach of the AI Act seems to have been appreciated by both academia and practitioners in the AI field[417].

On the other hand, the proposal has been described as "a science fiction inspired legislation"[418]. The criticism on the proposed AI Act stems from various angles. From a data protection standpoint, the EDPS-EDPB has expressed several key criticisms regarding the proposed AI legislation raging from lack of acknowledgment to personal data protection, to substantially criticising Article 5 of the proposal which prohibits certain AI systems. In this regard, the EDPB-EDPS has expressed concerns that Article 5 risks limiting the scope of the prohibition in a way which could turn the prohibition into being "meaningless" in practice due to an unclear definition of risk[419].

Furthermore, some authors criticise the Artificial Intelligence Act's rules for high-risk systems due to ex ante conformity assessment carried out by the providers themselves and the fact that the current AI standardisation process, which is mostly concentrated in the hands of the private sector, does not facilitate an inclusive AI standardisation system which reflect European values and fundamental rights[420,421].

More so, the AI Act proposal is also criticised due to the lack of an effective enforcement mechanism of legal rights and duties, stemming from facts that AI providers are given an inappropriately large role in the implementation of the regulation itself, with little actual role in the hands of the agencies, meaning the proposal fails to recognise the status of individuals adversely affected by the AI, including a complete lack of procedural rights, such as the right to seek redress or lack of compliant mechanism[422]. Similar criticism has led other researchers to conclude that "big tech emerges virtually unscathed under the new AI legislation despite being the object of widespread and growing concern"[423].

---

[416] Maria-Camilla Fiazza, 'The EU Proposal for Regulating AI : Foreseeable Impact on Medical Robotics' (2022).

[417] Martin Ebers and others, 'The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)' (2021) 4 J 2021, Vol. 4, Pages 589-603 589 <https://www.mdpi.com/2571-8800/4/4/43/htm> accessed 20 December 2021.

[418] Domenico Orlando, 'If Science Fiction Inspires the Law: Recent Examples with the EU Proposal for an AI Regulation' (2021) <https://limo.libis.be/primo-explore/fulldisplay?docid=LIRIAS3463286&context=L&vid=Lirias&search_scope=Lirias&tab=default_tab&lang=en_US&fromSitemap=1> accessed 14 December 2021.

[419] Jenny Bergholm, 'EDPB-EDPS Opinion: Four Lessons for the AI Regulation and Data Protection - CITIP Blog' (2021) <https://www.law.kuleuven.be/citip/blog/edpb-edps-opinion-four-lessons-for-the-ai-regulation-and-data-protection/> accessed 14 December 2021.

[420] Ebers (n 414).

[421] Mark Maccarthy and Kenneth Propp, 'Machines Learn That Brussels Writes the Rules: The EU's New AI Regulation' [2021] Brookings.Edu 4 <https://www.brookings.edu/blog/techtank/2021/05/04/machines-learn-that-brussels-writes-the-rules-the-eus-new-ai-regulation/>.

[422] Nathalie A Smuha and others, 'How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act' [2021] SSRN Electronic Journal <https://papers.ssrn.com/abstract=3899991> accessed 20 December 2021.

[423] Maccarthy and Propp (n 422).

6.3.3 Digital Health Technologies as High-Risk AI Systems in the AI Act Proposal

The AI Act proposal defines high-risk systems as systems which, irrespective of whether they are to be placed on the market, are "intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II"[424] of the proposed AI regulation[425]. For instance, in the case of the medical devices covered in Annex II of the AI proposal, where there are medical devices which have AI system as a safety component, or the AI system itself is a product, such products are required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II[426]. In respect of the latter, consider AI systems intended to be used to dispatch, emergency or first response services. The definition of the high-risk AI systems distinguishes between two categories of high-risk AI systems. The first category includes AI systems that are products or safety components of products that are already covered under harmonised EU legislation (Article 6(1)), such as medical devices, machinery, toys and so on. In this regard, the compliance mechanism under the AI Act would be somewhat "simplified", i.e., requiring only the special requirements for high-risk systems contained in section 4.4 to be observed and included as part of the present conformity assessment procedures for medical devices, as contained in Articles 24 and 43(3) of the proposal. The second category refers to standalone AI systems, as per Article 6(2), Annex III, that pose a severe risk of harm to the health and safety or an impact on the fundamental human rights, as enshrined in Article 7 of the proposal[427]. As to the latter category, the Commission has identified several such high-risk standalone systems such as biometric identification or credit scoring.

It should be further noted that the proposal contains essential requirements for high-risk AI systems in Title III, Chapter 2, before such systems are put on the European market. If adopted in its current format, these requirements would become mandatory and include the creation of a risk management system (Article 9), quality assurance criteria for training AI and testing data (Article 10), technical documentation (Article 11), record-keeping (Article12), transparency and user information (Article

[424] The European Parliament Proposal for a Regulation of the European Parliament and of the Council laying dow harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts COM/2021/206 final (n 15).

[425] ibid.

[426] The European Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (n 413).

[427] ibid.

13), human-machine interface tools that would ensure human supervision of the system (Article14), and obligations concerning the accuracy, robustness, and cybersecurity of systems (Article 15)[428].

In addition, the AI Act provides several innovations from a regulatory perspective which will affect big data-powered digital health technologies. From this perspective, this sub-section of the thesis analyses how the proposed AI Act may affect big data-powered digital health technologies and its implications to risk to privacy, data protection, and the right to health.

To start with, in the context of healthcare, the evolution of user-centric healthcare into personalised digitalised medical technologies that use various machine learning models and algorithms carries with it additional, privacy, and data protection risks, which must be balanced against the right to health. Such a balance is especially significant since privacy and data protection ought to be considered as a shared responsibility of health technology providers, manufacturers, developers, vendors, end users, and healthcare providers.

These risks are especially apparent in the cases of AI-run digital health technologies that may run afoul of sufficiently informed consents of data subjects, since they collect, process, and transfer sensitive personal data in unexpected ways without giving adequate prior notice, choices of participation, and other options[429]. Controversially, the very thing, i.e., data, we are trying to protect is also the thing that can be crucial to ensure the safety and effectiveness of such devices[430].

The case of the use of AI in digital health technologies that qualify as medical devices under MDR provides food for thought on how the existing regulatory regime, namely the MDR, and the proposed legislation on Artificial Intelligence will co-exist together. Consider, for instance, low-risk class I medical devices, such as smartwatches. In such devices, privacy might often prevail over the secondary use of personal data, while in the case of high-risk class III medical devices, such as defibrillators, the safety of medical devices might outweigh patient privacy[431].

Furthermore, from a privacy and data protection point of view, we may expect the AI Act to put an additional "burden" on the developers of AI health technologies. Developers will be required to consider not only privacy and security risks, but also ethical implications on security and privacy of their solutions on a broader scale. This additional "burden" takes the form of conformity assessments, namely CE marking, that AI providers would be obliged to conduct. The first conformity assessment would be required 'before a high-risk AI system is put on the European

[428] ibid.

[429] Timo Minssen and others, 'The EU-US Privacy Shield Regime for Cross- Border Transfers of Personal Data under the GDPR: What Are the Legal Challenges and How Might These Affect Cloudbased Technologies, Big data, and AI in the Medical Sector?' <https://papers.ssrn.com/abstract=3651094> accessed 23 June 2021.

[430] Janos Meszaros, Marcelo Corrales Compagnucci and Timo Minssen, 'The Interaction of the Medical Device Regulation and the GDPR : Do European Rules on Privacy and Scientific Research Impair the Safety & Performance of AI Medical Devices ? II . Collection and Processing of Health Data under the GDPR Modern Healthcare Sys' (2020) 3501545 1.

[431] ibid.

market', as enshrined in Article 43[432]. The second, is the post-market monitoring of AI systems that AI providers must undergo to "document and analyse the performance of high-risk AI systems throughout their lifetime, as enshrined in Article 61"[433] of the AI Act. In this respect it can be observed that the proposed conformity mechanisms highly are highly reminiscent of the Medical Device Regulation conformity assessment for regulated medical devices.

Furthermore, some authors argue that the proposed AI Act can be interpreted as a proposal to establish a "European wide ecosystem for conducting AI auditing"[434], a sort of assurance mechanism that is already widely used in other industries, such as IT security or financial services industries[435]. Such an ecosystem for conducting AI audits includes all different types of audits, for example, of the AI system itself, the AI provider's organisational audit, or ethic audit encouraging AI providers to draw up and apply voluntary codes of conduct under Article 69 of the AI Act. It can be observed that such AI audits would play a crucial role in ensuring that AI systems are ethically-sound[436]. AI audit mechanisms can play a positive role in both marketing and public relations[437].

The proposed AI Act assurance mechanisms do not directly link to compliance with the existing data protection frameworks to ensure compliance even though such systems, under the proposed act, are also required to guarantee compliance with any other applicable Union law. In this regard, any AI assurance mechanism, such as AI audits, would also have to be aligned and include data protection and privacy considerations (namely, the GDPR) to cover data protection and privacy risks. Such alignment of AI audits with the GDPR is crucial as AI providers may not be aware of all data protection or privacy risks which are highly dependent on the specific use of AI. Indeed, in its joint opinion on the AI proposal, the EDPS-EDPB "strongly recommended" "that the legislator includes a statement which confirms the applicability of the EU data protection legislation to processing of personal data within the scope of the AI Act"[438].

6.3.3.1 Integrating Regulated and Unregulated Digital Health Technologies with AI Regulation

[432] Floridi and others, 'Conformity Assessments and Post-Market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation' (n 402).
[433] ibid.
[434] ibid.
[435] ibid.
[436] The European Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (n 413).
[437] Jakob Mökander and Luciano Floridi, 'Ethics-Based Auditing to Develop Trustworthy AI' (2021) 31 Minds and Machines 323 <https://link.springer.com/article/10.1007/s11023-021-09557-8> accessed 14 December 2021.
[438] EDPB and EDPS, 'EDPB-EDPS Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)' 1.

Integrating the proposed AI Regulation into a well-established medical device regulatory regime will not be an easy task. Several observations with respect to the applicability of the proposed AI Act to the co-regulatory digital health technologies' regime should be made.

First, the proposed AI Act in terms of MDR may create regulatory ambiguity and regulatory overlap. For instance, under the current MDR practice, the manufacturer's intended purpose of the medical device produced is key when establishing regulatory applicability of the MDR. Similarly, the proposed regulation Article 3 (12) defines the concept of intended purpose as:

"the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation"[439].

The definition proposed in the AI Act mimics that of the MDR which establishes that intended purpose means "the use for which a device is intended according to the data supplied by the manufacturer on the label, in the instructions for use or in promotional or sales materials or statements and as specified by the manufacturer in the clinical evaluation"[440]. Therefore, the proposed AI Act establishes that the AI provider's intended purpose is king when establishing the applicability of the AI Act. Arguably, this may lead to an already existing problem in the digital health technologies' sector which we referred to in detail in Chapter 4 – explicit intended purpose versus implicit intended purpose, but in the context of AI applications.

Specifically, what occurs if the intended purpose established by the provider of the AI differs from the actual functionality of the AI? In the current proposal the answer to the issue remains unclear and is left unaddressed. It could be suggested that rather than merely focusing on the explicit intended purpose of the AI, the proposed regulation could also address the implicit purpose or the actual functionality of the AI system which, in turn, should be assessed by the Notified Body as part of the conformity assessment, in order not to significantly differ from the AI provider's claims.

The proposed regulation would need to be aligned with the already applicable regulatory requirements of regulated digital health technologies, i.e., medical devices, where such technologies also deploy AI systems. For instance, both the MDR in Annex I and the proposed regulation for AI, in Chapter 2, include general safety and security requirements both pre-market and post-market for their relevant technologies. Still, this is a great oversight by the legislators of the AI Act. The

[439] EU Commission Proposal for a Regulation of the European Parliament and of the Council laying dow harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts COM/2021/206 final (n 405).

[440] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/.

conformity requirements vary depending on the risk level assigned to the medical device, low to high risk, and the AI systems, minimal to unacceptable risk. It can be observed, however, that the pre-market and post-market requirements in both regulations overlap greatly. The draft of the AI Act currently remains silent on how the overlapping requirements in terms of the MDR will be addressed.

Also, there are instances where the regulatory conformity requirements differ between the two legislations. Most notable differences can be observed in the AI Act's additional requirements for conformity and documentation of AI systems. Such varying requirements include data and data governance established in Article 10, transparency established in Articles 11 and 53 of the AI Act, human oversight in Article 14, and accuracy and robustness in Article 15.

Researchers have long encouraged development of a system of transparent and distributed responsibility for digital health where all actors involved can be held proportionately and appropriately accountable for the safety of the patient at the end, not just the healthcare provider[441]. Such a system could be achieved through the development of appropriate regulatory norms, yet the MDR enforcement and accountability mechanisms remain questionable, especially when compared to a much more stringent regulatory regime, such as the U.S.[442]. Similarly, the proposed AI Act seems to fall short of establishing such mechanisms thus potentially slowing down further adoption of AI in healthcare.

The above cases have illustrated some of the most prominent implications of the proposed AI Act to the regulated digital health technology industry. Still, even the unregulated digital health technology industry, which is mainly based on digital consumer health devices, will be affected if (or rather, when) the AI Act is adopted. Nevertheless, rather than creating regulatory uncertainty for unregulated digital health technologies, the proposed AI Act should aim at providing clear and needed guidance.

In the context of unregulated digital health technologies, those falling outside the scope of the MDR, it can also be observed that the proposed AI regulation would impact such digital health technologies. For example, various consumer health applications that, for example, track menstrual cycles, sleep and fitness, and consumer wearable devices such as smartwatches and bands often deploy AI software and AI algorithms to provide insight. Since these technologies do not qualify under the MDR as a medical device, they still provide some sort of health-related functionality and processes user data. In this respect, the AI Act could be considered as a legal instrument that would ensure that such technologies safeguard the fundamental rights to privacy, data protection, and the

[441] Jessica Morley and others, 'The Debate on the Ethics of AI in Health Care: A Reconstruction and Critical Review' 1 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3486518#references-widget>.

[442] Jarman, Rozenblum and Huang (n 197).

right to health. Thus, having a potential impact on levelling the privacy, security, and safety of digital health technologies across the board.

The AI Act proposal is a strategically targeted regulation considering the envisaged growth of the AI system's market. The AI Act proposal attempts to achieve several different goals. First, the proposal attempts to ensure that AI systems entering the EU market are safe and respect existing laws on fundamental rights and EU values. To achieve the first goal, it proposes novel governance and enforcement mechanisms on fundamental rights and applicable safety requirements. Second, it attempts to be the cornerstone legislation in ensuring legal certainty in AI. Arguably, the proposal aims at facilitating the development of a single European market for lawful, safe, and trustworthy AI[443].

Additionally, "it seems fair to affirm that the aim of the law to govern the process of technological innovation should neither hinder its progress, nor require over-frequent revision to tackle such a process"[444]. Still, the newly proposed AI Act stresses the boundaries of non-hindrance of technological innovation due to regulatory overlaps with the existing regulations, creating regulatory ambiguities. At the same time, manufacturers and developers of digital health technologies that use or plan to use AI systems should begin to think of to how to address data governance, transparency, human oversight, accuracy, and robustness requirements of the AI they use. Likewise, the legislators of the AI Act should work on establishing a distributed responsibility framework for AI systems.

6.3.3.2 The AI Act Proposal and Digital Health Technologies in Public Health Emergencies: A Missed Opportunity?

To date, little research has focused on the potential implications of the proposed AI Act in the case of digital health technologies deployed in public health emergency scenarios. While the previous sections of the thesis provided an in-depth understanding of the relationship between the proposed AI Act and the digital health technologies regulatory landscape, this section focuses on digital health technologies in public health emergencies and how the proposed AI regulation will affect the deployment of such technologies. This section will therefore consider digital health technologies deployed in public healthcare emergencies, referring to the examples of Covid-19 pandemic deployed technologies.

---

[443] The European Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (n 413).

[444] Pagallo, Durante and Monteleone (n 361).

To start with, while the proposed AI Act presents itself as a horizontal regulation, it addresses the deployment of AI-based technologies in all types of emergencies, including health emergencies. Recital 37 of the proposed Act notes that, for example, "[…] AI systems used to dispatch or establish priority in the dispatching of emergency first response services should also be classified as high-risk since they make decisions in very critical situations for the life and health of persons and their property"[445]. In Annex III, on the subject of dealing with high-risk AI systems, Article 5(c) specifies that such first response systems will be classified as high specifically in the cases of "emergency first response services, including […] medical aid"[446]. The proposed AI Act has a limitedly addressed AI technologies used and deployed in healthcare emergencies, providing us with a single example, that is, the first response services which are classified as high-risk.

However, the proposed Act remains silent on the possible classification of AI systems, such as AI software used in other healthcare emergencies such as disease outbreaks or natural disasters that may affect public health and lead to public health crisis. For example, a severe draught in certain regions may lead to lack of food, starvation, and increased disease outbreaks. The deployment of AI systems (AI software in its own right or as part of a technology solution) would require the classification of such technology in terms of the AI Act. As noted in Recital 32 of the proposed AI Act, stand-alone AI systems would be classified as high-risk systems in cases where such pose the risk of harm to the fundamental rights of individuals, also "taking into account both the severity of the possible harm and its probability of occurrence and they are used in"[447]. Potentially, this means that the deployment of AI-based digital health technologies would need to be assessed by using the proportionality test between the risks to fundamental freedoms, as the right to privacy and data protection vis-à-vis the potential risk of harm if the technology is not deployed. Also, since such AI system is classified as a high-risk system, it would be required to undergo the conformity assessment procedure under the proposed AI Act, provided that no exemptions are applicable under the said proposal.

Furthermore, Article 54(1)(a)(ii) of the proposed AI Act states the processing of personal data for research and innovation (such as development of AI systems) for public interest, such as public health, or "disease prevention, control and treatment"[448] are permitted under the Act provided that such processing is carried out in the AI regulatory sandboxes[449]. This provision of the proposed AI

[445] The European Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (n 413).
[446] ibid.
[447] ibid.
[448] ibid.
[449] Article 53 of the proposed AI Act notes that the regulatory sandboxes are established AI regulatory sandboxes established "by one or more Member States competent authorities or the European Data Protection Supervisor"ibid.

Act aims to provide the possibility for the Member States to implement regulatory sandboxes that would facilitate the development of AI-based digital health technologies for public health emergencies. Nonetheless, its application is complicated to say the least.

Public health emergencies, such as the recent Covid-19 pandemic, showcased that their unpredictability requires a rapid and timely response and deployment of technologies to manage such emergencies. Precisely the time sensitive nature of public health emergencies is the crucial aspect that is overlooked by the proposed AI Act. Meaning that in case a public health emergency occurs, a timely deployment of an AI-based technology would be delayed as such technology would need to be 1. (potentially) developed to address the specific needs of an emergency, and 2. undergo a conformity assessment under the proposed AI Act, and any other applicable regulation. Concerning the first point, we should observe that currently, the understanding of public healthcare emergency technologies is broadly focused on the "known" public healthcare emergencies and technologies for managing various pandemics or disease outbreaks (again, the recent Covid-19 pandemic example showcased the spur in technologies that can be deployed in such a case), still overlooking all other "unknown" potential public health public crises, such as bio terrorism, biological toxins, or use of infectious agents. Therefore, in the case of another pandemic outbreak, the deployment of AI-based technologies such as contact-tracing applications may be swifter, as the application is already developed and would only need to undergo the AI Act conformity assessment. In a scenario of an "unknown" public health crisis, the development of AI-based digital health technology, especially that processes personal data, would be limited as it would need to be done in a regulatory sandbox established by the Member States, or the EDPS, which might not be available at the time of emergency. It also might be the case that even if such an AI regulatory sandbox is available, the technology has not been developed precisely due to the unpredictability of the nature of the public health emergency.

Considering the newest EU proposal for the Regulation on Serious-Cross Border Threats to Health, already analysed in Chapter 5 of the thesis, the proposed AI Act fails to address the scope of the applicability of the AI Act in terms of serious cross-border threats to health proposals. Specifically, under the proposal on Serious Cross-Border Threats to health, the ECDC will have increased powers, including the power to enable automated collection and surveillance of health data, media monitoring, and the application of AI for analysis and improvements of early preparedness for cross-border threats to health. The current scope of the AI Act fully applies also to the ECDC, subjecting the authority and the Member States' national competent authorities to a stringent regulatory oversight. Interestingly, the broad scope of the proposed AI Act and the lack of

addressing the interplay between the two proposals may limit the development of digital health technologies for emergency management as well as limit the use of data for the same.
Finally, taking the scope of the proposed AI Act into account, its potential treatment of healthcare emergency AI-based systems, and its interaction with proposal for the Serious Cross-Border Threats to Health discussed above, it may be concluded that the proposed AI Act is a missed opportunity to provide a streamlined approach to the processing of personal data that could facilitate innovation and development of new digital AI-based solutions for public needs, such as disease surveillance, and health risk management.

6.4 A Competitive Market: U.S. Approach to AI-based Digital Health Technologies

The United States Federal Drug Agency (the "FDA") is the main regulatory body that deals with the regulation and approval of medical devices, medical software, and medical or health AI in such devices. In 2019, the FDA proposed a plan for authorisation of AI in medical devices and medical software. In their, essentially, "whitepaper" the FDA proposed a predetermined change control plan for machine learning that includes a list of aspects the manufacturer intends to change through ML while remaining safe and effective[450]. This proposal aims at ensuring that ML and AI-based software as a medical device innovation and enhancements are not stalled due to regulatory inefficiency. Such inefficiencies may arise, for example, in situations where AI medical software that is being updated, because the update may change or introduce a new risk to the patient or cause significant harm would have to undergo the so-called "510K approval" mechanism, which can be rather lengthy.
Considering that machine learning and AI algorithms are constantly changing and learning, the FDA approach is to introduce a spectrum of AI and ML medical devices and software of medical devices. On the one side of such spectrum lies the so called "Locked Algorithms" with discrete updates where only the said algorithm is used within the medical devices or software as a medical device, notwithstanding the fact that AI or ML could improve such software as a medical device. On the other side of the spectrum lies what can be called "Continuously Adaptive Algorithms" with frequent updates, performed by a computer.
This approach includes a more relaxed regulatory regime for the "Locked-in algorithms" and a more stringent one for continuously evolving algorithms. Specifically, in the latter case the intention of the regulator is to include specifications requesting the manufacturer to include what

[450] 'Artificial Intelligence and Machine Learning in Software as a Medical Device | FDA' <https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device> accessed 21 July 2022.

aspects are to be changed through the use of AI or ML algorithms in a medical device as well as include explanation as to how these changes will affect safety, security, and effectiveness of the medical devices and, of the patient. These changes range from improvements in performance, such as, for example, the introduction of a new patient population where previously data was not available, thus potentially expanding the usability of a medical device. Nonetheless, authorisation would still be required for changes in, for example, initially- low risk software as a medical device using AI or ML where such changes would lead to high-risk of AI or ML. Take for example, a device taking skin images which then leverages the use of skin images for diagnostic purposes. The FDA takes the approach of a total product Lifecycle. Starting with 1. establishing good ML/AI practices And guiding principles[451]; 2. conducting a pre-market review for AI software as a medical device to ensure "reasonable assurance of safety and effectiveness and to continually monitor risks to patients throughout the lifecycle of their devices; and 3. ensuring monitoring through regulatory authorisation as necessary"[452]. In this step the FDA refers to the normal authorisation process as well as the new process for the AI/ML medical devices. In situations where the AI/ML medical device has already obtained an authorisation from the FDA with pre-approved changes and improvements for the AI/ML indicated by the manufacturer in the initial application stage and if such changes are not substantial or do not create new significant risks, there would be no need for a new authorisation process under the FDA regulations. On the other hand, in cases where AI/ML medical device changes are new, not pre-approved by the FDA, or carry significant risks, or put the AI/ML software into a new category of a medical device, or where the changes may introduce a new intended use of such AI/ML software as a medical device, the manufacturer would need to go through the standard authorisation process; 4. Real-world performance monitoring which would allow users and the FDA to continuously ensure safety and levels of effectiveness.

We should make several other observations of AI regulation within medical devices in the U.S. First, the FDA publishes a non-exhaustive list of AI/ML-embedded medical devices, open to the

[451] Similarly to the EU, the FDA has published "10 guiding principles which include: Multi-Disciplinary Expertise Is Leveraged Throughout the Total Product Life Cycle, good Software Engineering and Security Practices Are Implemented, Clinical Study Participants and Data Sets Are Representative of the Intended Patient Population, Training Data Sets Are Independent of Test Sets, Selected Reference Datasets Are Based Upon Best Available Methods, Model Design Is Tailored to the Available Data and Reflects the Intended Use of the Device, Focus Is Placed on the Performance of the Human-AI Team, Testing Demonstrates Device Performance during Clinically Relevant Conditions, Users Are Provided Clear, Essential Information, and Deployed Models Are Monitored for Performance and Re-training Risks are Managed"' FDA Releases Guiding Principles for Good Machine Learning Practice | American College of Radiology' <https://www.acr.org/Advocacy-and-Economics/Advocacy-News/Advocacy-News-Issues/In-the-Oct-30-2021-Issue/FDA-Releases-Guiding-Principles-for-Good-Machine-Learning-Practice> accessed 2 August 2022.. Further insight: https://www.fda.gov/medical-devices/software-medical-device-samd/good-machine-learning-practice-medical-device-development-guiding-principles

[452] 'Remote or Wearable Patient Monitoring Devices EUAs | FDA' <https://www.fda.gov/medical-devices/coronavirus-disease-2019-covid-19-emergency-use-authorizations-medical-devices/remote-or-wearable-patient-monitoring-devices-euas> accessed 14 September 2020.

public, making such information available to the public and increasing transparency also from the FDA's perspective, as a public body[453]. Second, the human-in-the-loop requirement[454] also falls under good AI/ML practices and guiding principles. In this case, the FDA notes that in developing AI/ML medical devices, human-in-the-loop and interpretability of the AI/ML algorithm considerations must be drawn up. This includes reflecting on aspects such as human factors when ensuring the safety of AI/ML devices and whether the person involved in this are suitable, have a level of experience and education or knowledge to address aspects such as automation bias. The FDA falls shorts of expressing how such human and AI interaction will develop and what manufacturers should address here, especially in cases where AI/ML algorithm might have an upper hand against humans in the interpretability of data. Third, the same good AI/ML practices and principles also include the requirement for the provision of clear and essential information to the users. This does not include what are the essential information is or how regularly such information should be provided.

This approach to managing the risks of AI and ML within the medical device industry is exceedingly different from the EU approach to AI and medical devices. The European approach to AI in digital health technologies and medical devices is based on the proposed AI Act which, if adopted in its current form, would create regulatory interplay and overlap as regards to the medical devices and its specific regulatory regime under the MDR[455]. This is especially important as the AI Act aims to be a horizontal regulation, applicable throughout all industries (similar to lex generalis), while the MDR is an industry-specific regulation (lex specialis). Yet, it could be observed that in the case of an AI medical device, the AI Act becomes lex specialis with the MDR being lex generalis, particularly as regards to the applicability of human oversight mechanism, provision of information to user and so on in terms of the AI Act requirements which are specific to the use of the AI.

6.5 Do the European Regulatory Initiatives Ensure the Rights to Privacy and Data Protection in AI-Powered Digital Health Technologies?

[453] The list is continuously updated and can be accessed at https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-aiml-enabled-medical-devices#resources

[454] 'Good Machine Learning Practice for Medical Device Development: Guiding Principles | FDA' <https://www.fda.gov/medical-devices/software-medical-device-samd/good-machine-learning-practice-medical-device-development-guiding-principles> accessed 21 July 2022.

[455] Elisabetta Biasin and Erik Kamenjašević, 'Cybersecurity of Medical Devices: New Challenges Arising from the AI Act and NIS 2 Directive Proposals' (2022) 3 International Cybersecurity Law Review 2022, Vol. 3, Pages 163-180 163 <https://www.scilit.net/article/f6fc072a0aa5803281f2e8f6da408f16> accessed 13 July 2022.

The interplay between the discussed European initiatives in the digital health technology sector with the proposed AI Act are undeniable, as they all attempt to enhance Europe's competitiveness in the digital market. Nonetheless, one question remains unanswered. Do all these European initiatives that establish a set of rules applicable to AI-powered digital health technologies ensure an adequate level of protection of the fundamental right to health with the rights to privacy and data protection in AI-powered digital health technologies? Considering the earlier analyses of the initiatives such as the European Health Union, the EU Digital Decade 2030, the creation of the Common EU Health Data Space, the European Data Strategy, and the proposal for the regulation of AI, this sub-section deliberates on this question and provides several observations.

First and foremost, the above-mentioned policies and regulatory initiatives create a network ecosystem of interwoven regulations that reinforce, rationalise, and clarify each other. The European initiatives create a remarkable degree of integration, as can be observed between the AI Act and the MDR, AI and the GDPR. This demonstrates a clear attempt to construct a genuine regulatory ecosystem. Such a regulatory ecosystem is aimed at creating regulatory certainty, which may be the key enabler for the flourishment of the AI-powered technologies in the single European digital market. Yet, it is a complex ecosystem that is becoming increasingly difficult to navigate even for an expert eye. The complexity of the regulatory ecosystem is particularly apparent at the contextual sector-specific level, such as the conformity assessment. At another level of abstraction, however, the European initiatives, such as the AI Act proposal, provide clarity on the legislative intent by establishing a scope and boundaries of permissible use of AI-powered digital health technologies based on risk. It also calls on the Member States to support AI regulation and innovation via regulatory testing, i.e., regulatory sandboxes.

An adequate level of protection to the fundamental rights to health, the rights to privacy, and data protection in AI-powered digital health technologies is achieved through all the levels of abstraction in the European initiatives. This can be observed from the analysis of the text on the European Health Union, the EU Digital Decade 2030, the creation of the EU Health Data Space, the European Data Strategy, and the proposed AI Act. For instance, the European Health Union was created with the goal of improving healthcare and health crisis management throughout the EU without hindering the right to privacy and the right to data protection. In fact, the EU Health Union initiatives, such as a proposal on the Serious Cross-Border Threats to Health regulation, which acknowledges that data protection and privacy principles must be observed where personal and sensitive data are processed, are enshrined in Article 26 of the proposal on Serious Cross Border Health Threats. Similarly, the EU Health Data Space proposal text acknowledges that European

values, such as the right to privacy and the right to data protection must be guaranteed in the EU Health Data Space.

Nonetheless, the protection of the right to privacy and data protection at the European policy-making level, the European regulatory initiative discussed, namely the AI Act proposal, paints a slightly different picture. The text of the proposed AI Act merely acknowledges the fundamental rights to health, privacy, and data protection, but does little in its current text to reconcile and balance these rights given the complex digital health technology sector. Fundamental rights are addressed generically in Title III of the proposal concerning the high-risk AI systems that may affect "health, safety, and fundamental rights"[456]. In this respect, it can be observed that the proposed AI Act is primarily based on the need to facilitate free movement within the EU rather than fundamental rights. In fact, the main legislative basis for the AI Act is contained in Article 114 TFEU, for the prevention of the fragmentation of the internal EU market. Similar observations on the lack of addressing risks concerning fundamental rights have been observed by researchers. In fact, some have noted that the proposal does little to reduce fundamental rights risks of the many systems not covered by Annex III (i.e., high-risk) and such a "'cliff edge' from some rules to practically none seems difficult to justify"[457].

To answer the question at the beginning of this section, the European policy and regulatory initiatives for the digital health technology sector reconcile the right to health with the right to privacy and data protection to some extent. In can be concluded that at the policy setting level, the reconciliation of these rights takes a more prominent role, while at the regulatory level such reconciliation takes a secondary role. Such an oversight may be caused due to the complex regulatory ecosystem surrounding AI-powered digital health technologies which should be rectified.

6.6 Conclusive Remarks

The chapter addressed and explored the importance of the current European policy and legislative proposals in the area of digital healthcare and digital health technologies from the perspective of the right to data protection and the right to privacy.

Based on the premise that the protection of the right to data protection and the right to health is achieved through legislative means, the chapter analysed three key European initiatives: the policy

[456] EU Commission Proposal for a Regulation of the European Parliament and of the Council laying dow harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts COM/2021/206 final (n 405).

[457] Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' <http://arxiv.org/abs/2107.03721>.

proposal of the European Health Union, the creation of the EU Health Data Space, and finally, the proposal for the regulation for the Artificial Intelligence.

Regarding the European Health Union, we observed that the proposal establishes a European health crisis governance system with the Covid-19 pandemic being a "favourable contextual condition"[458]. Consequently, it is observed that the envisaged European Health Union comes as a politically planned response to manage the public's disappointment regarding the Union's limited ability to respond to the Covid-19 pandemic, even with the crisis management mechanisms that were available.

As regards the EU Health Data Spaces, the protection of the fundamental rights to data protection and privacy will remain a battle. Even if the right to privacy and data protection are not absolute rights and may be limited, any limitations would however require a careful analysis. Therefore, it will be fundamental to establish detailed data management plans and policies could take a primary role as governance mechanisms to ensure legal access and processing of citizen personal data, in line with the GDPR. Additionally, the data governance mechanisms will take a prominent role in assuring a lawful, transparent, and ethical management of the data involved, including effective accountability mechanisms in the EU Health Data Spaces in cases where there are fundamental rights' implications. One key aspect concerning the EU Health Data Space is to reflect that such a space may become an instrument allowing for the better preparedness of future health-related crises.

Furthermore, the proposal for the regulation of Artificial Intelligence is a horizontal regulation laying down general rules for the use of AI. The legal analysis of the proposal indicates that the AI Act proposal is a strategically targeted regulation considering the envisaged growth of the AI system's market. It aims to achieve different goals: first, to ensure that AI systems entering the EU market are safe and respect existing laws on fundamental rights and EU values. To achieve the first goal, it proposes novel governance and enforcement mechanisms on fundamental rights and applicable safety requirements. Second, it attempts to be the cornerstone legislation in ensuring legal certainty in AI. Despite the goals it aims to achieve, the AI Act stresses the boundaries of non-hindrance of technological innovation due to regulatory overlaps with the existing regulations, creating regulatory ambiguities, that are particularly apparent in the area of digital health technologies and medical devices. Third, the AI Act proposal provides clarity on the legislative intent by establishing a scope and boundaries of permissible use of AI-powered digital health technologies based on risk. It also calls the Member States to support AI regulation and innovation via regulatory testing, i.e., regulatory sandboxes.

[458] Bazzan (n 369).

7 Guaranteeing the Right to Health and the Right to Privacy in Digital Health Technologies: Cybersecurity, Common Standards, and Certifications

Technology is eroding individual privacy at an unprecedented rate. Still, technology is also the instrument that can help individuals take back their privacy and data protection. While originally, privacy predominantly concerned intrusion into one's home, privacy in the cyberspace can be considered as a horizontal problem and is, in a sense, a "common denominator"[459] of various digital health technologies connected with the IoT or the IoE.

In fact, due to the ever-increasing interconnectivity of digital health technologies with the wider Internet of Everything, individual privacy and data protection in the cyberspace has become a collective responsibility, shifting from individual cybersecurity and privacy to "security of our society"[460].

Due to such interconnectivity and the increased threats not only to individuals but also to groups of individuals, and society at large in recent years, both the public and the private sectors have been pressured to step up their efforts exactly in the area of cybersecurity. Various actors have been called upon to balance the initiatives coming from non-governmental and private sectors in this regard. Likewise, it has been observed by scholars that today, national preferences and values play a decisive role in personal data protection regulatory future in Europe[461].

At the outset of this chapter, we should also observe that the concept of data protection, as acknowledged by scholars, overlaps with privacy in the digital space and can be often subsumed by the concept of privacy, under its umbrella[462].

The above pressures had its outcomes with cybersecurity promotion being transposed through various legislative initiatives in Europe. For example, the proposal for Network and Information Security (hereinafter the "NIS" and its follow up, the "NIS2") directives, the Cybersecurity Act.

---

[459] David Olivier Jaquet-Chiffelle and Michele Loi, 'Ethical and Unethical Hacking' (2020) 21 International Library of Ethics, Law and Technology 179 <https://serval.unil.ch/notice/serval:BIB_CB652A6CE0EC> accessed 2 August 2022.

[460] Lorenzo Pupillo, *EU Cybersecurity and the Paradox of Progress* (2018) <https://ssrn.com/abstract=3131559No2018/06,>.

[461] Pagallo, 'The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection' (n 151).

[462] Christof Koolen, 'Transparency and Consent in Data-Driven Smart Environments' [2020] SSRN Electronic Journal <https://papers.ssrn.com/abstract=3597736> accessed 6 April 2022.

These initiatives to secure data in the cyberspace are often accompanied by common certification and standardisation schemes coming from various private bodies, such as the International Organization for Standardization (hereafter, the "ISO").

Regarding cybersecurity in digital health technologies, the GDPR, being a technology-neutral regulation, endorsing self-regulatory instruments such as certifications and technical standards, could not have included specific certification and standardisation requirements for such technologies. In the context of the GDPR, the principle of technology neutrality infers that the protection of personal data should not depend on the technologies used for the processing of personal data as enshrined in Recital 15 of the GDPR.

At the core of the cybersecurity regulatory regime in the EU lie the NIS2 directive and the Cybersecurity Act, forming part of the EU strategic priorities established by the European Commission and High Representatives back in 2013. Such priorities include the development of "industrial and technological resources for cybersecurity by establishing a public-private platform on network and information security"[463] and facilitating the "development of security standards for technology 'with stronger, embedded, and user-friendly security features"[464]. These legislative acts also interact with digital health technologies' regulatory regime attempting to ensure an adequate protection of privacy and personal data in the digital space. For example, the principal European legislation on digital health technologies, namely the MDR, does not explicitly mention or address cybersecurity in its text.

Nonetheless, its guiding documents, the MDGC guidance, provides essential cybersecurity-related requirements that manufacturers ought to implement in digital health technologies qualifying as medical devices[465]. Specifically, the mentioned guidance provides that manufacturers will "set out minimum requirements concerning hardware, IT network characteristics, and IT security measures, including protection against unauthorised access"[466]. While the guiding document does not have a legally binding effect, being a soft-law instrument, on the manufacturers, it is the first of its kind of guidance by the European Commission on cybersecurity in digital health technologies and medical devices and is highly observed by the manufacturers of such technologies.

Considering the above, this chapter provides an overview of the European Union policies and regulatory measures adopted in the cybersecurity sector and their impact on big data and AI-

[463] Jaquet-Chiffelle and Loi (n 460).

[464] Gloria González Fuster and Lina Jasmontaite, 'Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights' (2020).

[465] For the complete list see: Medical Devices Coordination Group , Guidance on Cybersecurity of medical devices (Dec. 2019)

[466] I Glenn Cohen and others (eds), 'The Future of Medical Device Regulation: Innovation and Protection' <https://www.cambridge.org/core/books/future-of-medical-device-regulation/7ABD9575718C5F31B69E4CE00DD7F7E7> accessed 20 April 2022.

powered digital health technologies. By invoking a healthcare perspective, this chapter uncovers how the recent policy developments regulating cybersecurity guarantee the benefits of big data and AI in digital health technologies while ensuring the right to privacy and data protection.

This chapter is a consequence of a 6-month internship at an advisory company in Turin, Italy, focusing on developing various digital health technologies and providing audit services regarding various cybersecurity and privacy standards and specifications.

More concretely, the chapter starts by addressing the legislative developments in the area, namely the EU's Cybersecurity Act and its impact on digital health technology privacy. The chapter then examines how standardisation and certifications can be used as supportive mechanisms not only to ensure regulatory compliance, but also ensure preservation of privacy in digital health technologies without hindering the right to health. Lastly, the chapter analyses and examines the role of international standards in the fight to ensure data protection and privacy in the context of digital health technologies. Fundamentally, this chapter answers the following question: considering the risk to privacy and data protection in digital health technologies in public health emergencies, how can common standardisation and certification of digital health technologies introduce ramifications to such risks?

7.1 Privacy Preservation in Digital Health Technologies: Focus on the EU Cybersecurity Act, Standardisation, and Certifications

Due to ongoing digital transformation, it is imperative to guarantee that all deployed IoT and IoE devices ensure the highest standards of user privacy and security. Considering that such devices often have network access, cybersecurity of such devices has become of primary importance. Such security is particularly relevant in the healthcare industry which deals with personal and sensitive patient health data. After all, we live in times where, 'if your heart skips a beat, it might have been hacked' thoughts are a reality.

Thus, ensuring that the benefits of big data and AI-powered digital health technologies are taken advantage of by the healthcare industry while guaranteeing the right to privacy and data protection is essential. In the opinion of the author, this can be achieved using legislative means such as the EU Cybersecurity Act[467] (hereafter, the "Act") and through the application of supporting mechanisms such as relevant common standards and certifications.

[467] Full name: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

In fact, in 2018, the European Union Agency for Cybersecurity (hereafter, "ENISA") published a report on the security certification opportunities in the healthcare sector, which underlined the need for an acceptable level of privacy of digital health technologies for all stakeholders to ensure trust in such electronic services and products. The said report reached a focal conclusion that "it is impossible to certify the healthcare sector as a whole"[468] due to the different requirements used in medical devices, the Internet of Medical Things, IoT, various sets of data and so on. The only way forward, according to ENISA, is to create synergies across various certifiable areas to reduce the amount of over-certification.

In this respect, the EU Cybersecurity Act may be called one of the EU's attempts to create such synergies. It is also a step forward to address the so-called "paradox of progress" referring to the society's increased efficiency due to digitalisation, while at the same time also becoming more fragile due to the increased cybersecurity risks[469]. The Cybersecurity Act was proposed by the European Commission in 2017 and adopted by the EU Parliament in 2019. The Cybersecurity Act's scope establishes detailed "objectives, tasks and organisational matters relating to ENISA"[470] in Article 1(a).

In a nutshell, the Cybersecurity Act strengthens ENISA's duties and rights by granting the agency a permanent mandate and providing ENISA with financial and human resources required to achieve a high-level European cybersecurity. Still, the actual core of the Act focuses on the establishment of the first, common European-wide cybersecurity certification scheme framework for various ICT products as enshrined in Article 8 of the Cybersecurity Act. Such a framework aims to ensure a common approach to cybersecurity in the European internal market and, ultimately, aims to improve cybersecurity for the Internet of Things. The establishment of the common cybersecurity certification scheme by ENISA is a leap forward in the cybersecurity area for the EU and is discussed in detail below, from the perspective of privacy in digital health technologies.

In relation to data protection, GDPR Article 43 acknowledges the importance of standardisation and certification as self-regulatory tools in the IoT. Technical standards are not simply good practices but are considered by the GDPR as means to ensure a data controller's compliance and adequate level of personal data protection. Similarly, standardisation and certification based on standards are

---

[468] ENISA and others, 'ICT Security Certification Opportunities in the Healthcare Sector' (2018) <https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications%250Ahttps://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications/%250Ahttps://www.enisa.europa.eu/publications/healthcare-certificat>.

[469] Pupillo (n 461).

[470] OJ L 151, Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) 2018 15.

recognised as tools to achieve privacy by design and by default, enshrined in Article 25 of the GDPR.

7.2 Common Cybersecurity Certifications for Digital Health Technologies

As acknowledged in Recital 67 of the Cybersecurity Act, cybersecurity certifications of ICT products and devices is currently used to a limited extent[471]. Often, ICT product and device certification occurs only where the Member States have implemented a national framework of usually industry-driven certification schemes. Also, it is observed that existing certification schemes present significant shortcomings and differences that often impede mutual recognition of certifications within the Union[472]. Therefore, the adoption of a common approach for a European-wise certification framework that lays down the main horizontal requirements for certifications schemes is essential to prevent the internal market fragmentation.

However, cybersecurity certifications to ensure personal data privacy and security in various healthcare devices is not an entirely new topic. In 2018 ENISA published a report on ICT certification opportunities in healthcare considering the Internet of Medical Things and its interconnection with the wider IoT and IoE. Already in 2018, it was observed that security issues in healthcare include the lack of privacy in healthcare systems. For example, emergency messages that are sent in clear text and which include potentially sensitive data.

At the same time, it was observed that in some healthcare scenarios "safety issues prevail over ICT security"[473]. A simple example of this convergence can be found if a smartphone carries out a function of a medical device. In the event of a critical fault, smartphones are programmed to shut down, while a digital heart pacemaker cannot do that; instead it must enter the so-called "safe mode" and continue functioning. Hence a convergence between security and safety is paramount to ensure human lives[474].

We note that security and privacy requirements are already built into regulated medical devices themselves, following security and privacy by default and by design principles before such devices are placed on the EU internal market. In fact, in the third IoT Security Conference dedicated to IoT held in October 2020, ENISA noted that in the IoT, security measures should follow the principle of security by design and by default for all products and services.

---

[471] ibid.

[472] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) 2019 15.

[473] ENISA and others (n 469).

[474] ibid.

Still, the gap of unregulated digital health technologies' cybersecurity and privacy remains a matter of debate. To address the gap between the regulated medical device industry, the mHealth possibilities, and the health ICT sector, through the powers granted to ENISA under the EU Cybersecurity Act, ENISA has formed several interest groups to address and establish EU-wide security certification standards that would cover all products and services. In June 2020, ENISA announced the creation of the Stakeholders Cybersecurity Certification Group (henceforth, the "SCCG"), which advises ENISA on strategic issues regarding cybersecurity certification that are market driven and help to reduce fragmentation between various existing schemes in the EU Member States. Likewise, to facilitate standardisation throughout industry, ENISA encourages the use of already industry-approved and used cybersecurity standards such as ICO/IEC 27001 to ensure an adequate level of protection regarding cybersecurity, privacy, and data protection.

It can be observed that security by design and by default is tremendously significant in IoT and IoE devices used in healthcare sector, especially ones that are placed on the internal EU market. The leading motive for such prominence is the sensitive nature of healthcare IoT and IoE devices collected and stored data, and the impact it may have on an individual's well-being if such devices are under attack. Such a need to safeguard the sensitive health-related data is also enshrined in Article 9 of the GDPR that lists health related data as a special category of data, requiring enhanced protection.

The adoption of the Cybersecurity Act in 2019 facilitated the starting point for the creation of common European certification framework for various ICT products and devices put on the EU internal market. From the user of IoT and IoE devices perspective, the Cybersecurity Act aims at protecting the users of digital products, processes, and services through the establishment of the EU-wide certification of such technologies.

In this respect, the Cybersecurity Act provides that certification and standardisation are two of the methods that can be used to ensure the security and privacy of users and personal data. Nonetheless, certification and standardisation are not new mechanisms incorporated into the European legislative frameworks.

Since its inception, standardisation has meant the inclusion of essential requirements and voluntary adoption of harmonised standards which would provide a "presumption of conformity" with EU legislation[475]. As stated earlier, standards and certification such as ICO/IEC from private bodies are the go-to industry standard to ensure cybersecurity and data protection.

[475] Claude Scheuer and others, 'European Integration through Standardisation: How Judicial Review Is Breaking down the Club House of Private Standardisation Bodies' (2013) 50 Common Market Law Review 145 <https://research.tilburguniversity.edu/en/publications/european-integration-through-standardisation-how-judicial-review-> accessed 16 December 2021.

Nevertheless, the use of standards and certifications is also highly criticised. For instance, Matus and Veale observe that current standards are "meta-standards" focused on common terminology and networking aspects rather than focusing on a more comprehensive approach that includes provision of additional information to consumers (referred to as "credence qualities"), especially considering the use of Artificial Intelligence systems[476].

Title III of the Cybersecurity Act may act as the tool to move away from such "meta-standards" and towards a comprehensive European cybersecurity certification framework. Requirements enshrined under Title III of the Cybersecurity Act require the Commission to provide a "rolling work programme for European cybersecurity certification"[477], indicating strategic priorities of certification schemes which shall be prepared by ENISA.

Furthermore, Articles 51 to 56 of the same Act contain the core of the EU cybersecurity certification schemes. First, Article 51 provides that the security objective of certification schemes shall, inter alia, include the protection of stored, transmitted or otherwise processed data. Such data includes personal and sensitive data, against a myriad of risks such as unauthorised processing, storage, disclosure, destruction and so on.

Second, Article 52 then provides assurance levels of the European cybersecurity certification schemes: basic, substantial, and high. These assurance levels are proportionate to risk levels of associated ICT products and devices in terms of risk probability and impact. In other words, the Cybersecurity Act deploys a risk-based approach to cybersecurity. Depending on the assurance level, different certification requirements would apply accordingly[478].

Third, Article 53 provides a voluntary conformity self-assessment with European cybersecurity certification schemes for ICT products with a basic assurance level, carrying a low risk of security threats[479]. Fourth, Article 54 then provides specific details on the elements of cybersecurity certification schemes. Article 55 of the Cybersecurity Act includes, at least to some extent, a provision that requires the manufacturers of ICT and IoE devices to provide end users with additional information on cybersecurity, which was lacking in previous certification and standardisations schemes as observed by Matus and Veale earlier in the thesis. In this respect, the Cybersecurity Act requires manufacturers to make public the following data:

---

[476] Kira JM Matus and Michael Veale, 'Certification Systems for Machine Learning: Lessons from Sustainability' [2021] Regulation & Governance <https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12417> accessed 16 December 2021.

[477] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance).

[478] OJ L 151 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) (n 471).

[479] ibid.

a. “guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ICT products or services;
b. the period during which security support will be offered to end users, in particular as regards the availability of cybersecurity related updates;
c. contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers;
d. a reference to online repositories listing publicly disclosed vulnerabilities related to the ICT product, ICT service or ICT process and to any relevant cybersecurity advisories”[480].

While the above information does not specifically address information to end users regarding the use of artificial intelligence, such would presumably fall under information disclosure requirements of the proposed AI Act, thus providing additional and arguably useful information to end users. Finally, Article 56 establishes that certification schemes will be “voluntary, unless otherwise specified by Union or Member State law”[481]. In the digital health technology sector, the common certifications should not be considered optional, especially for medical devices and digital health technologies that use networks.

It should be observed that the certification schemes referred to in the Cybersecurity Act are expected to be made available through the implementing acts which would allow developers to voluntarily apply for third-party certification or a conformity self-attestation by the manufacturers for products that present a low level of risk. Moreover, an observation should be made that the Commission has the right to assess whether mandatory certification is required for certain categories of products and services. To date, no such mandatory certification requirements have been published (apart from those that are already covered by industry specific legislation). Though, we can expect that certain crucial sectors, such as healthcare, may be subject to mandatory certifications.

Consequently, the Cybersecurity Act acts as a backbone for the EU-wide tool which would facilitate a higher level of cybersecurity and a level of protection for a user’s privacy and data protection throughout all industries. Considering digital health technologies and the medical device industry, the provision of common standards and certification mechanisms could facilitate a faster adoption of secure digital health technologies. However, no common standards for certifications on the cybersecurity of digital health technologies have been issued so far by the Commission.

[480] ibid.
[481] ibid.

7.3 Certification and Standardisation Under the AI Act Proposal: Impacting Digital Health Technologies?

To address the issue of trust in artificial intelligence powered technologies, Chapter 5 of the AI Act proposal enshrines standards, conformity assessment, and certification for high-risk AI systems[482]. Article 40 of the proposal provides that such high-risk AI systems, which are already in conformity with harmonised standards (or parts of such standards) and which have been published in the Official Journal of the EU, shall be presumed to be in conformity with the proposal's requirements, to the extent those standards cover those requirements[483]. Meaning that AI technologies, such as medical devices, which already conform with harmonised standards at the EU level, would have presumed conformity regarding the proposal's harmonised standard, to the extent that the same requirements are covered under the obtained certification. The requirements that are specific for AI, would need partial conformity with harmonised standards. Likewise, Article 42(2) of the proposal enshrines that:

"high-risk AI systems that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 <…> and <…> which have been published in the Official Journal of the European Union shall be presumed to be in compliance with the cybersecurity requirements set out in Article 15 of this Regulation insofar as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements"[484].

It can be envisaged that digital health technologies that use AI would also fall under the above scenario, whereas it would have to apply for multiple certifications under different regulatory frameworks, to the extent these are not already covered by an obtained certification. For example, in a healthcare scenario, the EU currently recognises ISO 13485:2016 as the common standard for

---

[482] "High-risk AI systems" are defined in the AI Act proposal article 6(1): "AI system shall be considered high-risk where both of the following conditions are fulfilled: (a) the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II;
(b) the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II.
2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk."

[483] The European Commission Annexes to the Proposal for a Regulation of the European Parliament and of the Council Laying down harmonised rules on Artificial Intelligence (Artificial INtelligence Act) and amending certain union legislative acts (n 410).

[484] EU Commission Proposal for a Regulation of the European Parliament and of the Council laying dow harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts COM/2021/206 final (n 405).

medical devices quality management systems which includes requirements for regulatory purposes. ISO 13485:2016 focuses on medical devices that fall under the MDR and as addressed above, similar requirements could be also applied in the case of other digital health technologies, that do not qualify as a medical device. It should be noted that only a few ISO standards have been recognised under the EU implementing acts as common standards for digital health technologies and those that were recognised focus on specific matters such as quality or safety of such devices, however, they do not address privacy or data protection directly.

Interestingly, presumed conformity will only be approved if the standards are EU official standards, excluding third-party standardisation schemes such as the above-mentioned ISO schemes. While the EU is pushing its own agenda of standards (most of which are yet to be published), the ISO organisation has also begun a process of developing new standards for AI. Namely the ISO 23894, known as the "AI Risk Standard", ISO/IEC 23053:2022, a framework for AI systems using machine learning, whilst also working together with IEC at a joint committee (SC 42) to develop international standards on AI. It may be considered that ISO and IEC are taking "first to the market" approach to AI standards and certifications which would be based on the AI Act's requirements, thus beating EU common standards for the same. Whether such approach will work, we are yet to find out.

7.4 Cybersecurity Standards, Guidelines, and Third-Party Certifications for Digital Health Technologies: Multi-layered Relationship

While ENISA is still working on EU-wide standardisation and certification schemes, the guaranteeing of big data and AI-powered digital health technologies benefits and ensuring that privacy and data protection is also guaranteed may also be achieved through the application of industry-accepted standards of digital health technologies. As observed above, standards play a crucial role in the cybersecurity certification scheme for IoT, and IoE products as observed by ENISA.

In essence, standards can be understood as functional and assurance requirements for products, services or technologies that provide consistency among such product, service, or technology developers, and that serve as an industry-approved metric to establish and measure such product security and privacy. Standards often range from guidelines for development, documents and updates on best practices, or specifications on interoperability and, are often voluntary. For example, in 2015, "the European Commission issued the first standardisation request to the European Standardisation Organisations to develop privacy management standards based on Article

8”[485] of the EU CFR, indicating that standardisation is a form of co-regulation in the case of data protection.

Typically, standards include general techniques on how to protect user data in cyber space and other environments, in and outside organisations, or when data is stored, or in transit. Standards, as understood today, focus on reducing the risk of cyber-attacks and data leakages for organisations or developers of products or services. Standards can include policies, security techniques, guidelines, risk management approaches, staff training, technologies, or best practices. For instance, the digital health device industry has long followed global standards set by the International Organization for Standardization (henceforth, ISO), which are considered the gold standard and industry’s best practices. Similarly, some of the medical devices may follow the international standards for digital health technologies that use electronic and related technologies set by the International Electrotechnical Commission (henceforth, the “IEC”).

Likewise, when it comes to assessing security concerns in technologies, including digital health technologies, the choice of standardisation and certification mechanisms expands enormously. As can be observed in Figure 1 below, currently there are 436 certifications listed (data as of April 2022) regarding security assessment that covers different aspects of the technology deployment stage. Figure 1 covers a security assessment roadmap, encompassing various privacy and data protection-related issues ranging from communications and network security, security architecture, Security and Risk Management to security operations and incident reporting.

[485] Irene Kamara, ‘Co-Regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation “Mandate”’ (2017) 8 European Journal of Law and Technology <https://www.ejlt.org/index.php/ejlt/article/view/545/723> accessed 21 January 2022.

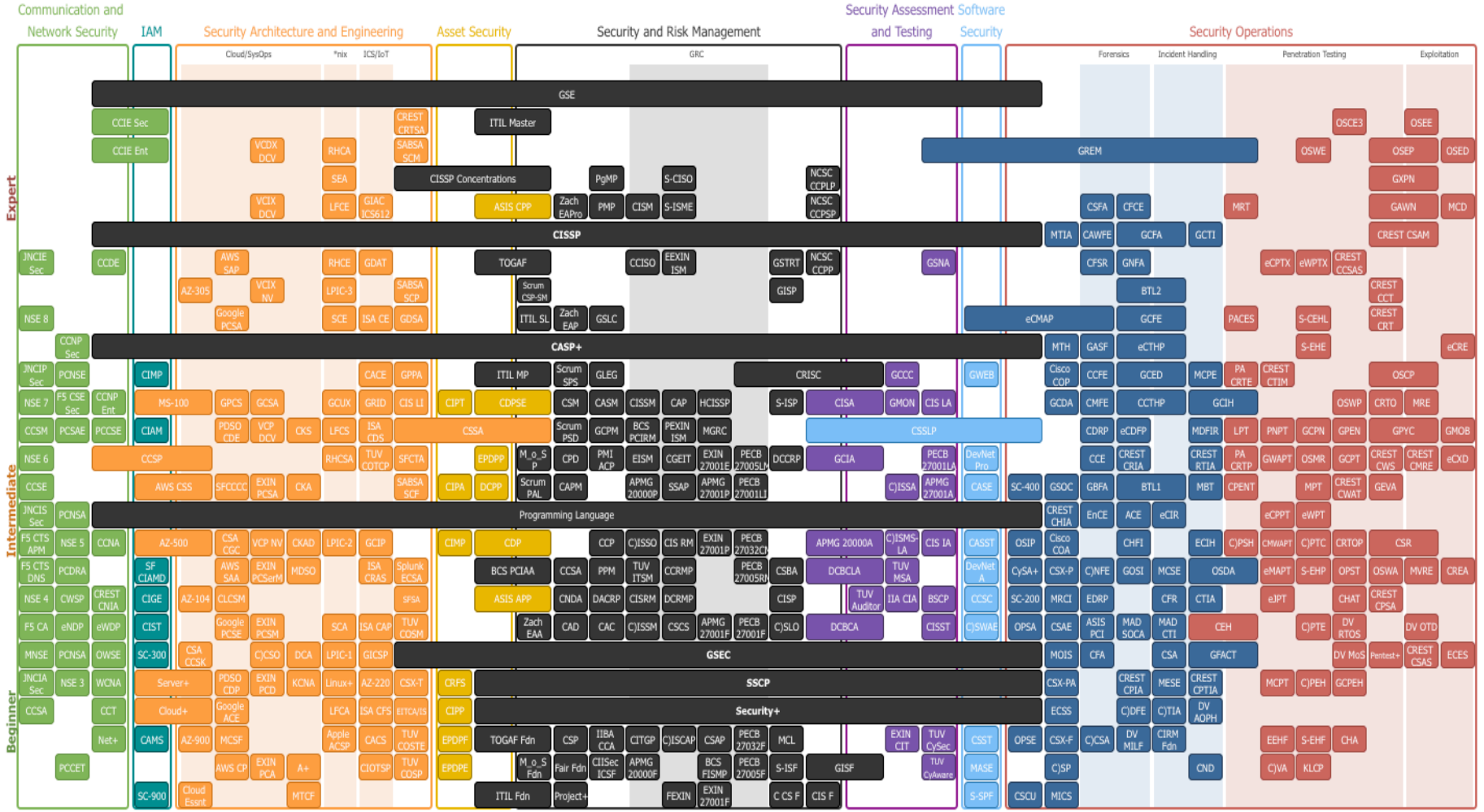

Figure 1 Security Assessment Roadmap. Source: https://pauljerimy.com/security-certification-roadmap/

7.4.1 ISO Cybersecurity Certifications for Ensuring Privacy in Digital Health Technologies

In the healthcare sector, ISO and IEC certifications and standards are most often applied. Quintessentially, ISO standards and certifications are internationally recognised standards that ought to help companies establish a level of homogeneity regarding product development, management, and provision of services. Regarding digital healthcare technologies, ISO standards tend to concentrate on controls of processes within an organisation that establish a level of compliance quality, safety, and, to some extent, regulatory compliance in terms of such devices' privacy. IEC standards, instead, focus on the manufacturing and testing of such devices' safety and security. However, there is no exhaustive list of standards and certifications for digital health technologies, as certifications and standards often depend on the health technology at hand[486]. For instance, from a privacy and data protection perspective, digital health technologies ought to apply ISO standards within the ISO 27000 standard family such as the ISO 27001, which covers information security management systems, or ISO 27002, which provides guidance to implement the necessary security measures[487]. It should be noted that the ISO 27001 standard controls that can be found in Annex A are derived and aligned with the ISO 27002 standard that deals with information security, cybersecurity and privacy protection — information security controls. Specifically, it provides best practices for information security management systems and is based on the cybersecurity's CIA triad: confidentiality, integrity, and availability.

Perhaps the most important standard in terms of privacy and data protection is the above-mentioned ISO 27701 on personal information security management systems (in terms of the standard known as "PIMS"), as updated and published in 2019. It should be observed that ISO 27701 is not a healthcare-specific standard as it is not restricted only to healthcare platforms or medical devices, but rather it is a general standard that can be applied within different industries, products, and services. Considering that the demand for data protection tools such as standards and certifications has been growing, and which have often remained

[486] Some establish a list of "must-have" ISO certifications and standards for the medical industry in general. Such as: https://isoupdate.com/general/iso-certifications-in-the-medical-field-the-must-have-standards/ ; however, such lists often come from industry experts and private companies providing certification services rather than governmental bodies within the healthcare industry.

[487] 'ISO 27701, an International Standard Addressing Personal Data Protection | CNIL' <https://www.cnil.fr/en/iso-27701-international-standard-addressing-personal-data-protection> accessed 2 August 2022.

scarce, the introduction of the ISO 27701 standard came at the right time[488] as it allowed organisations and DPOs to assess their compliance, at least partially, to the GDPR.

Considering that data protection and privacy are a pre-requisite for digital health technologies, the ISO 27701 standard can be described as the "go-to" standard in relation to ensuring privacy and data protection for all digital health technologies. The standard is of a particular importance in the healthcare industry where medical devices are being connected to the larger IoT and IoE network and higher risks related to data breaches, systems hacks, and personal healthcare information loss arise.

Specifically, the ISO 27701 defines the personal information management system and security requirements for the processing of personal data, which is defined as "Personally Identifiable Information"[489] or PII, for short. The said standard allows organisations to enhance their data protection measures by improving their cybersecurity and information security management. In particular, the said ISO standard covers specific aspects related to the processing of personal data, such as the determination of an organisation as a data controller and/or processor (in the language of the standard referred to as "PII controller" and "PII processor" respectively)[490] or requirement for a unified risk management and a designation of a Data Protection Officer (in terms of ISO 27701 called "privacy officer") which corresponds to Article 38 of the GDPR. Also, a requirement for privacy by design and by default is also enshrined in the standards which also transposes requirements under Article 25 of the GDPR concerning data protection by design and by default.

Requirements for data transfers, including compliance with regulations and laws are also mentioned by the standard. Such compliance includes the fundamental principles regarding the purpose of processing, the legal basis for processing, consent, collection, withdrawal, also reminiscent of the principles relating to the processing of personal data under Article 5 of the GDPR.

---

[488] As observed by some authors, some 45 schemes have been developed in a period of less than two years to address the growing demand of certifications in terms of GDPR articles 42 and 43.Eric Lachaud, 'ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification' (2020) 6 European Data Protection Law Review 194.

[489] It should be noted that the list of PII definitions under the ISO and personal data, under the GDPR, are defined differently. PII under ISO specifically refers to a list of PII that is to be protected whilst the GDPR's definition of personal data is broader and less construed. It could therefore be argued that the GDPR's notion of personal data covers more data types than that of PII for the purposes of ISO certifications. This in turn limits the applicability of the ISO certifications specifically for GDPR purposes, as one may fall short if they only applied ISO standards in order to comply with data protection legislation.

[490] The European Parliament and The Council Regulation (EU) 2016/679 of the European Parliament and 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 (n 9).

Furthermore, the standard also includes detailed requirements concerning data and an organisation's role in such processing, that are enshrined in the GDPR. Such requirements include, for instance, data subject rights, such as right of access, erasure, correction, automated decision making, data sharing, and data transfers.

Although ISO 27701 offers operational advantages, such as being a widely accepted industry standard, its uptake by organisations could threaten GDPR Articles 42 and 43 implementation by imposing "ISO's approach to the EU supervisory authorities"[491], that may promote two competing frameworks with conflicting approaches[492].

ISO standards are voluntary standards and fall outside the monitoring of ISO organisation. ISO itself does not certify conformity or compliance with its published standards, as such certifications are open to any third-party conformity assessment body proposing such services, often known as certification schemes. Thus, questioning whether third-party conformity assessment bodies can ensure adequate certification to such schemes, being privately owned entities focusing on profits.

When compared to the ISO standardisation and certification schemes, the GDPR's Article 42 and 43 standard setting and their implementation monitoring has been set by the regulator and requires a regulatory scrutiny. The GDPR Articles 42 and 43 establish that any recognised certification scheme at the European level aims at demonstrating compliance with the applicable EU data protection framework. These harmonised technical standards at the EU level would become part of the EU law as already established by CJEU in 2016 James Elliot Construction case[493,494,495].

Also, considering that ISO certifications is a "free market" where various players can enter and provide such services, such market players also set prices for certifications with ISO standards that may not be accessible to small or medium-sized enterprises[496]. A certification at the EU level instead, would be accessible to all organisations irrespective of its budget. Considering the divergent approaches and implementation of the ISO standards and GDPR

[491] Lachaud (n 489).

[492] Lachaud (n 489).

[493] 'A Harmonised European (Technical) Standard-Provision of EU Law! (Judgment in C-613/14 James Elliott Construction) – European Law Blog' <https://europeanlawblog.eu/2017/01/24/a-harmonised-european-technical-standard-provision-of-eu-law-judgment-in-c-61314-james-elliott-construction/> accessed 16 June 2022.

[494] *Case C-613/14*.

[495] Arnaud Van Waeyenberge and David Restrepo, 'James Elliot Construction : A " New (Ish) Approach " to Judicial Review of Standardisation' [2017] European Law Review.

[496] It should be noted that third-party assessment bodies do not always issue an ISO certification seal as it is a practice that is combatted by the ISO. Instead such bodies provide an attestation of conformity that an organisation has applied a particular ISO standard.

requirements for establishing such standards, finding a way forward to a common European approach will remain essential.

In this regard, the EU Cybersecurity Act offers interesting possibilities considering certifications for data protection and privacy. The EU Cybersecurity Act could work as means of establishing an overriding policy on EU-wide standards and certifications schemes for the purposes of the GDPR[497]. This is made possible under Article 8 of the Cybersecurity Act, which empowers ENISA with the "development and implementation of policy on cybersecurity certifications"[498] and under Article 46 which enshrines that a "cybersecurity certification framework shall be established in order to improve the conditions for the functioning of the internal market"[499]. Article 48 of the same Act enshrines powers to the Commission to request ENISA to prepare a cybersecurity certification framework.

Until such EU level certification schemes are adopted, for the time being the ISO 27701 standard remains as the way to incorporate the best cybersecurity, privacy, and data protection practices for digital health technologies by the developers of such technologies, allowing the risks associated with privacy and personal data protection to be minimised through enhancing cybersecurity measures. According to CNIL (the French Data Protection Authority), the ISO 27701 standard's proximity with the GDPR is "materialised in a specific annex that maps each clause of the standard with the corresponding GDPR article"[500]. Still, it is and remains a global standard that is "not GDPR specific, nor does it constitute, as such, a GDPR certification instrument as described in Article 42 of the regulation"[501]. Indeed, if the ISO 27701 standard were applied on its own, for example, in the case of medical devices, it would not constitute compliance with GDPR from a regulatory standpoint. Rather, as observed by CNIL, ISO "represents the state-of-the-art in terms of privacy protection and will allow organisations adopting it to increase their maturity and demonstrate an active approach to personal data protection"[502].

---

[497] Lachaud (n 489).

[498] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance).

[499] ibid.

[500] 'ISO 27701, an International Standard Addressing Personal Data Protection | CNIL' <https://www.cnil.fr/en/iso-27701-international-standard-addressing-personal-data-protection> accessed 16 June 2022.

[501] ibid.

[502] ibid.

7.4.1.1 Data Protection Specific Standards and Certifications

While ISO 27000 family standards may ensure partial compliance with Europe's data protection laws regards privacy and cybersecurity of data, in recent years, the industry has also seen an increase in developments of specific standards that ensure GDPR compliance[503].

According to the study by the University of Tilburg, as many as 117 certification schemes focusing on data protection had been set up as of 2018. Amongst the identified data protection certification schemes, the Italian ISDP0003 Data Protection Certification scheme is an accredited certification scheme and has been recognised by the study as one of the top five EU-wide, "all GDPR model (comprehensive)" GDPR certification schemes[504,505]. Just like ISO certification schemes, the ISDP 10003 scheme is a voluntary scheme, applicable to all types of organisations, services, and products that process personal data. It is a self-regulation instrument that focuses specifically on GDPR compliance. Thus, its standards and requirements for certification stem directly from the GDPR enshrined rules.

The ISDP 10003 sets out requirements such as levels of accuracy, timeliness, credibility, principles of quality, security, secure management, compliance of the management regarding the processing of personal data, specifically referencing correct risk management when dealing with personal data.

Structurally, the ISDP 10003 standard is similar to the ISO standards, making it easier to navigate for specialists. For example, the structure of said standard starts with introduction, scope, normative references, which then lead to terms and definitions[506]. The ISDP 10003 standard takes a risk-based approach to compliance with data protection (likewise, the ISO 27000 group standards also use risk-based approaches).

When compared to the GDPR, the GDPR prioritises a fundamental rights approach while at the same time incorporating some aspects of risk-based approach, such as the GDPR certification enshrined in the regulation. Such an all-embracing approach provides a win-win solution for both protecting fundamental rights but also allowing secure data processing practices within the organisation.

---

[503] Further information can be accessed at: https://research.tilburguniversity.edu/en/publications/data-protection-certification-mechanisms-study-on-articles-42-and

[504] Irene Kamara and others, 'Data Protection Certification Mechanisms: Study on Articles 42 and 43 of the Regulation (EU) 2016/679. Final Report' (2019) <https://ec.europa.eu/info/sites/info/files/data_protection_certification_mechanisms_study_final.pdf>.

[505] 'L'European Commission Promuove ISDP©10003' <https://www.in-veo.com/it/news-it/461-l-european-commission-promuove-isdp-10003> accessed 27 June 2022.

[506] The structure of the standard partially follows High Level Structure (HLS) standard and ISO/IEC 17065

In terms of specific requirements, when compared to ISO 27000 family standards, both ISDP 10003 and ISO 27000 family standards require controllers to evaluate the "inherent risk (RI)[507] by means of objective parameters"[508]. Likewise, the processor or the controller must also assess whether "the residual risk (Rr) […] can be considered under control"[509]. Also, both the controller and processor under the said standard are required to analyse in advance the source of risk related to personal data processing activities and have a risk policy in place.
However, this is where the similarities end between the two above-mentioned standards. The real difference between the two standards lies in the methodology chosen for the standards. The ISDP 10003 standard methodology are the GDPR norms and the requirements arising for certification, which are the scope and the purpose of the said certification scheme. On the other hand, the methodology and the scope of the ISO 27000 standards focuses on general privacy and cybersecurity aspects and does not focus specifically on the GDPR compliance.
In essence, the ISDP 10003 defines its general scope of application in accordance with Article 42(1) of the GDPR and the scope of the standard is of a general nature, applicable to all controllers and processors who process personal data, regardless of the processes, products, or services provided or sold[510].
The definitions that the ISDP 10003 uses are taken from the GDPR and other ISO standards such as ISO 27001 and ISO 27002. For example, personal data in ISDP 10003 is defined as "any information relating to an identified or identifiable natural person"[511]. The standard also contains definitions of identification data, genetic data, biometric data, and special data which includes data revealing racial or ethnical origin, religious beliefs and so on, reminiscent of special categories of personal data, a term used in the GDPR. Some definitions, such as data concerning health are equivalent to the GDPR-enshrined terms, whilst other definitions are a combination of ISO and GDPR terminology[512].
The standard implements a process approach, i.e., processes that are considered for the evaluation of personal data processing. These processes in the ISDP 10003 standard correspond to the GDPR compliance requirements. For example, GDPR Articles 5 and 6 enshrine personal data processing principles, such as lawfulness, which are transposed into

[507] Related to the processing activities
[508] InVEo, 'International Scheme For Assessing Compliance with European Regulation 2016/679: ISDP 10003-2020 Rev00 En.Pdf' (2020).
[509] ibid.
[510] ibid.
[511] ibid.
[512] See for further detail InVeo ISDP 10003 standard definitions section

the ISDP 10003 standard requirements under A.1, A2, and A3 relating to principles applicable to processing of personal data.

As for the GDPR compliance, the ISDP 10003 standard sets out that the controller is responsible for making decisions regarding the processing of personal data, including implementing adequate safeguards for such processing, while the processor "must be able to demonstrate compliance with the European Regulation (author's note: the GDPR) and with the requirements of the controller"[513]. The standard then sets outs control objectives applicable to both the controller and the processor. Such control objectives include 7 macro-objects, which reflect compliance to the GDPR:

1. Implementing appropriate policies for personal data protection processing (7.2 and Annex A.1) as required under GDPR Articles 5(2) and 24.
2. Subjects involved in the processing (Annex A.2). Amongst these are basic principles for processing as enshrined in the GDPR, such as the controller's, joint controller's, processor's, and DPO's responsibilities as required under the GDPR Articles 4(7), 4(8), 28, and 38.
3. Principles applicable to the processing of personal data (A.3) which include accountability, purpose of processing, data minimisation, retention of data, fairness and transparency, lawfulness of processing, including consent, rights of the data subject, information provision and so on. Control objectives set out in this requirement also correspond to the GDPR principles and requirements enshrined in Articles 5 (1), 6 (1), 7 (1-3), 8(1), 12 (1) of the GDPR
4. Evaluation of products' or services' data protection by design and by default (A.4.). This macro-requirement allows an organisation to demonstrate the controller's and processor's compliance through adjustments and changes to its processes during the design stage, including, for example, default minimisation settings or adoption of data protection by design policies. The control objectives set out in this macro-objective largely correspond to the GDPR Article 25 requirements.
5. General obligations, risk management and personal data security (A.5.) corresponding to the GDPR requirements set under Articles 24, 30, 33, 34, and 29. The obligations under this category include mapping categories of personal data to be processed, preparing necessary records for processing, storage, and access to records. Said obligations include several security measures, such as the prevention of loss of data,

[513] InVEo (n 509).

the requirement to have a system administrator (same as ISO), ensuring adequate policies and procedures in the event of data breaches and communication of such to the data subject. The security obligations are also supported by organisational measures for personal data protection (similarly as for ISO 27001). These include risk assessment, security policy preparation, coordination, risk evaluation, treatment, mitigation, training, and awareness. Interestingly, the general obligations also include technical measures for personal data protection such as pseudonymisation, encryption, anonymisation, restriction to access, and application of national standards for confidentiality.

6. Impact assessment requirement. Under the ISDP 10003 standard, we also find methodology for carrying out a DPIA and the requirements for the carrying out thereof, in line with the GDPR.
7. Finally, in line with the GDPR, the ISDP 10003 standard have specific objectives in cases of transfers of personal data to third countries and cloud computing[514] (A.7.). Specifically, it requires an assessment of whether the controller has complied with the requirements under the GDPR for such transfers and the legal basis for such transfer based on binding corporate rules. It does not, however, consider the last Schrems II decision and its findings when requiring controls for third-country transfers. As regards to cloud computing, the control objectives include risk evaluation, reliability of the provider, contractual clauses, physical location of servers, data retention times, cloud service security. These requirements largely correspond to requirements set out in Articles 29, 32, 45, 46, and 47 of the GDPR.

Apart from private, third-party certifications focusing on the GDPR, in June 2022, the Luxembourg National Data Protection Commission ("CNPD") became the first EU Member State to adopt a GDPR certification mechanism, known as the GDPR-CARPA[515].

The outcomes of such GDPR-specific certification models should be considered. First, the ISDP 10003 being a multi-sector certification model allows an organisation's GDPR compliance for all business activities to be assessed. Second, the standard applies to all processes allowing certification of conformity with all systems and processes dedicated to personal data. Third, being a self-regulation mechanism, the ISDP 10003 provides an EU-wide model of GDPR certification and can be applied by an international organisation which

[514] Particularly important considering Schrems II decision by the CJEU.

[515] 'The CNPD Adopts the Certification Mechanism GDPR-CARPA | European Data Protection Board' <https://edpb.europa.eu/news/national-news/2022/cnpd-adopts-certification-mechanism-gdpr-carpa_en> accessed 30 June 2022.

carries out personal data processing activities in or outside the EU. Also, as an accredited certification scheme, falling withing the scope of the GDPR Article 42, the ISDP 10003 standard, while with its limitations, is a one-fits-all GDPR certification solution which, from an economics' point of view. could benefit small and mediums sized enterprises (SMEs), ensuring their compliance with the GDPR without being exceedingly costly for such enterprises.

Finally, certification schemes such as the GDPR-CARPA, being government-approved schemes, may mark the shift in the GDPR certification schemes across the EU, which focused on private standardisation schemes, and encourage the use of official government approved certification schemes. While private third-party certification schemes will still play a role in certification of data protection compliance, organisations will now have a wider choice in certification schemes that will facilitate competition within standardisation and certification market, especially considering costs of such certifications for small and medium-sized enterprises.

7.4.2 Standardisation and Certification of Digital Health Technologies in Public Health Emergencies

Besides the ISO 27000 family of standards concerning privacy, data protection, and cybersecurity of various products, several other standards should be examined. Although such standards do not directly deal with personal data, they address privacy issues of digital health technologies in a broader sense.

For example, standard ISO 13485:2016 for quality management ensures a high-level of user information protection, safety, and security of devices, while ISO 14791:2019 covers medical device risk management, and ISO 62304:2006, which focuses on standards for software used in medical devices. Particularly in the medical device industry, standards such as ISO 13485:2016 standard ensures medical device manufacturer's quality of systems to test their devices at all stages of production, including the design phase.

In terms of healthcare emergencies, certain ISO certifications also cover healthcare "informatics, interoperability of public health emergency preparedness and response

information systems, business rules, terminology, and data vocabulary"[516]. However, such standards are currently under development[517].

Specifically for public healthcare emergencies, such as the Covid-19 pandemic, ISO has also made available several standards free of charge, to assist the management of the Covid-19 pandemic in coordination with IEC. Most of the standards made available on the market focused on the development of medical equipment, such as standards for masks and other relevant healthcare devices, or tools or health and safety standards. A few other readily available standards also focus on security and resilience, and risk management.

Of a particular interest is the standard ISO 31000:2018, which deals with risk management within organisations. The risks within the framework of this standard are defined broadly and cover operational risks, such as privacy and data protection. Since the standard is generic, and does not apply within one industry, it allows organisations also in the healthcare industry, such as Covid-19 application developers, to assess risks related to loss or unauthorised access to data within the organisation itself.

These standards, as mentioned above, do not directly address privacy or data protection, nonetheless they form a crucial part of the overall security requirements for digital health technologies such as medical devices, also supported by the MDR, and at the organisation level.

Also, the IEC 60601 standard may be applied to digital health technologies as it covers safety and essential performance of medical electrical equipment. Similarly, IEC 62304:2016 is a functional standard and is referred to and used for medical device software design safety and maintenance of software. Developers of medical devices mostly follow such standards as they provide a baseline for a medical devices' cybersecurity, data protection, and privacy framework.

Other ISO standards are currently being developed and will focus on standards for personalised digital health, thus further expanding the common standardisation and certification framework for digital health technologies[518]. We are still to uncover whether the

[516] 'ISO - ISO/CD 5477 - Health Informatics —Interoperability of Public Health Emergency Preparedness and Response Information Systems –Business Rules, Terminology and Data Vocabulary' <https://inacal.isolutions.iso.org/standard/81303.html> accessed 2 August 2022.

[517] ISO, 'ISO - ISO/CD 5477 - Health Informatics —Interoperability of Public Health Emergency Preparedness and Response Information Systems –Business Rules, Terminology and Data Vocabulary' <https://www.iso.org/standard/81303.html> accessed 17 June 2022.

[518] 'ISO - ISO/AWI TS 6201 - Health Informatics — Personalised Digital Health -Framework' <https://www.iso.org/standard/82107.html> accessed 13 January 2022.

new standards will address privacy and data protection risks specifically in digital health technologies.

A few final observations should be made as regards to the use of standardisation and certification in digital health technologies deployed in various public health emergencies. Often, health emergencies are highly time sensitive situations that require prompt intervention. For example, the Covid-19 pandemic required EU and the Member States to be more prepared to manage a pandemic, a preparedness that extended past national borders. The deployment of technologies, such as contact tracing applications, was a time sensitive matter. The management of the spread of the Covid-19 virus, as well as the collection of data for public authorities, and research to be able to prepare the necessary treatments and vaccinations, were of utmost importance.

Considering the time sensitivity of public health emergencies, the application of standards and certification to technologies developed in emergencies is debatable. One the one hand, if a deployed digital health technology processes personal data, ensuring the highest levels of data protection is often best achieved using supplementary tools such as cybersecurity standardisation and certification.

On the other hand, precisely the time sensitivity of such public health emergencies may preclude governments and organisations from implementing the standard best industry practices in the development of such digital health technologies, as certification mechanisms are time consuming to obtain. Since the use of such standards and certifications remains voluntary to date, this to some extent addresses the conundrum. Still, considering that standardisation and certification may become obligatory in the future for certain technological solutions (for example, particularly ones that use AI and that may be deployed in health emergencies), the regulator would need to consider certain derogations regarding the deployment of digital health technologies in various public healthcare crises. These derogations would need to widen their scope to cover a wide range of public healthcare emergencies, covering not only the "known" technologies deployed in the Covid-19 pandemic, Ebola, or Zika outbreaks, but also facilitating the deployment of digital health technologies for the yet "unknown" public health crises.

7.5 Between Europe and the U.S.: Diverging Approaches to Standardisation and Certification of Digital Health Technologies

While the above-mentioned standards at an international level, standardisation at a national level should be also addressed, especially considering the competing jurisdictions for innovation such as the United States. The U.S. has been considered as a leader at establishing nationwide standards for certification of various products and services. The FDA regulates the medical devices industry, considering cybersecurity and technical aspects of such devices are delegated to other federal agencies[519]. Specifically, the U.S. National Institute of Standards and Technology (henceforth, the "NIST") issues its own guidance and standards for medical and other healthcare technologies. For example, NIST issues guidance and standards on security for first responder mobile and wearable devices or security for implantable medical devices, as well on securing electronic health records on mobile phones.

In the current U.S. regulatory regime, the FDA, along with other government agencies such as the NIST, are closely monitoring medical devices at every stage with regards to their efficacy, security, and safety[520]. In fact, as early as 2005 the FDA recognised the importance of ensuring cybersecurity in digital healthcare technologies and medical devices by providing guidance to the industry on Cybersecurity for Networked Medical Devices Containing Off-the-Shelf ("OTS") Software[521]. NIST then expanded on this framework with further guidance through the years, including promotion "security by design" approaches, and guidance on interoperable medical devices cyber vulnerabilities, including threats to data. This federal guidance by both agencies serves as "excellent conceptual frameworks" as they map out existing manufacturing design processes to align them and provide a consensus standard, such as the FDA's endorsed standard developed by the Association for the Advancement of Medical Instrumentation ("AAMI") TIR57 and UL 2900 series[522].

It should be observed that both the FDA and the NIST work hand in hand to ensure timely and relevant publications and guidance to digital health technologies manufacturers, also considering use of emerging technologies such as the AI or quantum computing[523].

---

[519] We should note however, that the FDA directly deals with the approval of AI medical software through either a 510K mechanism ("medium risk" AI medical devices), where the modification of software may change or introduce a new risk to the patient or cause significant harm. FDA however focuses on significant risks to health and safety of the patient rather than the cybersecurity, as discussed in Chapter 6 in more detail.

[520] Bernhard Lobmayr, 'An Assessment of the EU Approach to Medical Device Regulation against the Backdrop of the US System' (2010) 1 European Journal of Risk Regulation 137 <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/abs/an-assessment-of-the-eu-approach-to-medical-device-regulation-against-the-backdrop-of-the-us-system/2080FE575590A8DCB51DB513AEF75BCA> accessed 26 July 2022.

[521] Scott Anderson and Trish Williams, 'Cybersecurity and Medical Devices: Are the ISO/IEC 80001-2-2 Technical Controls up to the Challenge?' (2018) 56 Computer Standards & Interfaces 134.

[522] ibid.

[523] While this falls outside the scope of the thesis, it should be observed that NIST has published guidance, for example, on the use of AI in medical devices and research. Please consult for further reading:

Therefore, streamlining the U.S. approach to cybersecurity standardisation in the healthcare industry to ensure that manufacturers can implement guidance and conform with the applicable rules and regulations.

As a competitive market, Europe, with ENISA's task to provide a common cybersecurity certification framework for technologies in IoT and the IoE can be said to be in competition with the U.S. standardisation bodies. Europe does not currently have common cybersecurity standards and certifications for digital healthcare devices to date.

Rather, in healthcare domain, digital health technologies and medical devices including digital health devices' developers are encouraged to follow the Medical Device Coordination Group's (the "MDCG") issued guidelines. In the context of digital health technologies that fall under the category of medical devices, privacy and cybersecurity measures of such devices are addressed by the MDGC 2019-16 guidance on cybersecurity of medical devices that is supported by the MDR. The MDR itself (Annex I) only incorporates some of the cybersecurity requirements into the EU regulatory framework for digital health technology privacy, as observed in detail in Chapter 4, providing a partial harmonisation within the regulated medical devices' industry.

The MDGC guidance, however, focuses on other cybersecurity aspects that "are not explicitly mentioned in the Medical Device Regulation"[524] itself regarding medical devices completing the base privacy and cybersecurity framework applicable to medical devices. Still, it is also specified that certain "requirements regarding privacy and confidentiality of data associated with the use of medical devices that may be outside the scope of the MDR but are subject to other legislation"[525]. For example, as in case of confidentiality requirements between patients and doctors, or data protection requirements falling under the GDPR scope. While the MDGC issued guidelines that are not legally binding to its members, they are mostly observed, and it could be argued that such guidelines could be adopted as the industry's best practices for digital health technologies that are unregulated, such as, for example, mHealth or eHealth technologies.

Similarly, to the MDGC guidelines, the digital health technology industry is also guided by the International Medical Device Regulator's Forum (the "IMDRF") and the IMDRF's draft published principles and best practices for medical devices' cybersecurity standards. The aim

---

https://www.nist.gov/artificial-intelligence; Also, as observed by Scott Anderson and Trish Williams in 'Cybersecurity and Medical Devices s: Are the ISO/IEC 80001-2-2 Technical Controls up to the Challenge?' (2018) 56 Computer Standards & Interfaces 134, the FDA and NIST have been instrumental in providing guidance on cybersecurity and security by design in medical IOT.

[524] Medical Device Coordination Group (n 231).

[525] ibid.

of such publications is to further promote a globally harmonised approach to medical device cybersecurity and to provide cybersecurity guidance for all stakeholders across the device lifecycle[526].

A noteworthy feature vis-à-vis digital health technologies and innovative health technology sector in Europe should be noted. In January 2022, the European Commission regulation 2021/2282 on Health Technology Assessment came into force. The said regulation is aimed at "improving the availability of innovative technologies in the area of health, such as medical devices"[527]. The regulation, which is set be applicable as of January 2025, ensures efficient use of resources and strengthens the quality of healthcare technology assessment across the Union, by providing an innovative framework for health technology assessment at the Union level[528].

The proposed regulation itself does not define what is considered an innovative health technology; however, it includes a definition of the health technology assessment that is to be understood as a "multidisciplinary process that summarises information about the medical, patient and social aspects and the economic and ethical issues related to the use of a health technology in a systematic, transparent, unbiased and robust manner"[529]. This means that health technologies that undergo such a valuation would undertake a multidisciplinary assessment before being approved for launching on the internal EU market. The newly adopted regulation is also aimed at providing "information about medical, economic, social and ethical issues related to the use of a health technology"[530].

The regulation focuses primarily on the clinical effectiveness and safety of the health technologies. Still, the text of the regulation remains vague on the specificities of such assessment and further complicates an already complicated digital health technology landscape. Its essentiality will require developers of certain (digital) health technologies to undergo another compliance exercise to receive a CE marking.

To add an additional layer of complexity, in the growing health IoE model, AI-based digital health technologies further require enhanced data privacy and security standards and certifications. In this respect the primary focus is on the 2018 established European Technical

---

[526] ibid.

[527] The European Commission, 'Health Technology Assessment Regulation' <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6771> accessed 13 January 2022.

[528] European Commission Regulation (EU) 2021/2282 of the European Parliament and of the Council of 15 December 2021 on health technology assessment and amending Directive 2011/24/EU (Text with EEA relevance) PE/80/2021/INIT (n 378).

[529] ibid.

[530] 'Q&A: Adoption of Regulation on Health Technology Assessment' <https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_6773> accessed 19 May 2022.

Standards Organisations (henceforth, the "ETSI") and the European Committee for Electrotechnical Standardisation (henceforth, the "CEN" or "CENELEC"). Currently, both ETSI and CENELEC primarily focus on the standards relating to AI security, privacy, and ethics for EU oriented AI solutions[531]. The development of standards in these three key areas is crucial, especially considering the future adoption of the proposal for the EU AI regulation that also incorporates digital health technologies.

While certification and standardisation have taken a prominent role in the EU when ensuring that innovative technologies, including digital health technologies, comply with the EU legislation, they do not come without criticism. Both the certifications and standards on which the EU tends to rely so greatly have their limitations. The limitation regards the concern of over-reliance on such certifications and standards. Considering the private nature of standardisation and certification bodies, there is no guarantee that the established standards, even in cooperation with EU certification bodies (which, at the moment, have published very limited standards and certifications for digital health technologies), will comply with EU values and rights. As rightly observed, "standards should not be instrumentalised to shift regulatory power to private actors"[532].

To add to all this, the voluntary nature of certifications and standards provides the right for organisation to choose between the standards to apply, how to apply them and to what extent to comply with them, indicating the possibility of selecting standards or certifications to suit the needs of private corporations rather than those reflecting, for instance, EU values.

7.6 Conclusive Remarks

This chapter presented and explored how European legislative proposals and existing legislation in the cybersecurity area further consolidate personal data protection and privacy in Europe. The protection of the fundamental rights as observed in the chapter is also achieved through the establishment and use of common technical standards and certifications for digital health technologies, as supportive mechanisms to regulatory tools already available.

[531] Automated Decision Making, 'Global Attitudes AI , Machine Surveillance as Towards a Service Learning & Automated Decision Making The European AI-Assisted Mass Surveillance Marketplace Surveillance as a Service'.

[532] 'Feedback from: ETUC' <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13099-Standardisation-strategy/F2663296_en> accessed 24 January 2022.

The chapter paid particular focus on the Cybersecurity Act, ISO and IEC established certifications and standards, as industry's set best practices. The chapter first carried out an analysis of the EU Cybersecurity Act from the perspective of data protection and digital health technologies. By firstly highlighting the broad material scope of the EU privacy law, we pointed out that privacy law does not only cover the GDPR, but also encompasses supporting and sectoral legislation such as the EU Cybersecurity Act, the NIS2 directive, accompanied by supportive industry specific measures, such as guidelines (e.g., the above-mentioned guidelines on medical devices), and common standards and certification requirements in different industries.

The analysis of the above-mentioned legislation led to a first conclusion that there is a complex relationship between ensuring privacy and data protection in digital health technologies. Ensuring these fundamental rights is achieved via the establishment of an EU-wide legislative framework, i.e., the EU's Cybersecurity Act, and through supporting technical guidelines, standards, and certifications that, when assessed altogether, ensure that risks associated with the use of big data and AI are considered and addressed vis-à-vis the right to privacy, and data protection.

The chapter also established that private, third-party standards and certifications on privacy such as the ISO 27000 family standards, while being industry accepted best practices, fall short on establishing conformity with specific GDPR requirements. Yet, we have also established that the certification industry has moved forward and has put forward GDPR specific standards and specification schemes, such as the ISDP 10003 or the Luxembourg's GDPR-CARPA certification scheme, focusing specifically on the GDPR compliance. Thus, there is no single certification mechanism that fully incorporates both privacy compliance aspects and provides GDPR compliance. Therefore, a mix of both privacy certification schemes and GDPR specific certification schemes should be used to ensure overall privacy and data protection within digital health technologies.

8 Conclusions

This thesis examined big data's impact on digital healthcare technologies, placing a particular focus on the examples of digital health technologies deployed in public health emergencies, from a legal standpoint. More precisely, it studied the standard legal stance that a balance between the right to privacy and the right to health should be ensured when deploying digital healthcare technologies in various healthcare scenarios.

The thesis strived to grasp how different regulatory mechanisms ensure fundamental rights to privacy and data protection without hindering the fundamental right to health in the case of healthcare crisis. At the same time, the thesis aimed to understand the pitfalls of the regulatory mechanisms deployed, and the potential technical and legal ways to move forward in this respect. The research also deployed several case studies regarding the use of digital health technologies in healthcare emergencies and such technologies' approach to personal data protection and privacy in a digital world. The following sections set out the findings of this thesis.

8.1 Review of Background and Problem Questions

This research sought to appreciate and investigate digital health technologies in the digital world from the perspectives of health and privacy laws.

While the right to privacy has long existed in our societies, the right to personal data protection was first introduced as a way to consolidate the individual right to privacy due to unprecedented technological developments in the late 1970s and onwards. With the creation of a digital world and a digital society, one thing became clear- an individual's information is as important as the rights associated with it. The right to personal data protection in a digital society became the basis of a whole regulatory ecosystem regarding the processing of an individual's personal data and his/her rights to other fundamental human rights, such as the right to privacy, non-discrimination, and even the fundamental right to health.

Similarly, the right to health, which was first enshrined in the 1948 Universal Declaration on Human Rights, gave the push to the establishment for the fundamental protection of the right to health. The European Convention on Human Rights in this regard became the leading legal instrument to ensure the right to health with its legally binding effects on the Old Continent.

While both the right to health and the right to privacy appear in the above-mentioned declarations, their interaction was limited and relatively unexplored until the shift into the digital world. Indeed, it can be observed that the technological revolution happened

somewhat outside the healthcare industry, with big strides forward being taken in the last ten years to catch up with the other industries.

Considering the large amounts of personal and sensitive health data available for processing from various healthcare actors, the need to provide improved and more patient-centred healthcare, while ensuring that patient data is secure, remains a topical subject.

From an analytical standpoint, the thesis aimed to provide three-fold contributions:

1. With a specific focus on big data, the research contributes to literature regarding the analysis and conceptualisation of big data and its relationship with digital health technologies. In this regard, the research examined what constitutes big data, digital health technologies, and healthcare emergencies under the current regulatory regimes in Europe. This analysis portrayed accurate image of the complexity of the topic in interdisciplinary research. Since the heart of the thesis stands with legal analysis, the thesis focused on the analysis of the notions in health law, such as the MDR, data protection laws such as the GDPR, fundamental rights declarations, the technological meaning of the terms, and discussed the state of the art by employing examples from the healthcare sector.

2. Focusing on the selected issue of ensuring the right to privacy, data protection, and the right to health, the research contributed to the examination as regards the effects on such rights considering the deployment of digital health technologies in the peculiar scenario of healthcare emergencies. The thesis considered an example of Covid-19 pandemic management technologies and their effects on the right to privacy, data protection, and the right to health. In this respect, the research examined how privacy and data protection were achieved by both legal and technical means in the Covid-19 technologies deployed. Two case studies were analysed. First, an analysis of contact-tracing applications vis-à-vis quarantine applications was carried out, from the perspective of privacy and data protection. In the case of the contact tracing applications, the GDPR served as the basis for government authorities in the Member States to assess that the technological solutions ensure privacy and data protection. This was achieved by the requirements to carry out and the publish a Data Protection Impact Assessment on such contact-tracing applications. Based on the GDPR, the EDPS and the EDPB ad hoc guidance on the contact-tracing technologies, such guidance provided the desired clarifications on the processing of personal and health data in times of pandemics to developers and governments on how to ensure

data protection and privacy in the times of crisis. Finally, we observed that the deployment of digital health technologies in times of crisis and their impact on fundamental rights to privacy and data protection depends greatly on the technology deployed, the jurisdiction it is deployed in, and the cultural, economic, and sociological aspects surrounding a particular jurisdiction the technology is deployed in.

The thesis also analysed the EU Digital Green Certificate, as the EU's unified approach to health crisis management. In this respect, the thesis established that the balance between the right to health and the rights to privacy and data protection, when deploying digital health technologies in public healthcare emergencies, was ensured by employing the existing regulatory regimes. The GDPR played a fundamental role in ensuring that the EU Digital Green Certificate is aligned with data protection principles and norms. It was observed that in this case too, ad hoc guidance provided by the EDPS served its purpose and provided the necessary supervision to government authorities in the deployment of the EU Digital Green Certificate in line with the data protection requirements. Finally, the CJEU has also played a role on deciding whether the government measures limiting personal freedoms during the Covid-19 pandemic were balanced in the light of other fundamental rights involved, as has been observed by the recent cases in the Court on the subject-matter (e.g., the discussed Zambrano case).

3. Shifting focus from a legal analysis on the Covid-19 technologies, the research contributed to literature on AI-based digital health technologies and common standardisation and certification schemes. Specifically, the thesis examined how the current regulatory proposal on AI will affect the right to privacy and data protection in regulated digital health technologies and healthcare emergencies. The thesis established that incorporating new rules on AI into an existing digital health technology regulatory regime will be no easy task. This is particularly evident as an overlap between the AI Act's proposed norms and the ones enshrined in the MDR may arise. What is more, the research observed that the AI's Act missed an opportunity to ensure that AI can be deployed in a timely manner in a time-sensitive health crisis, which requires an immediate response. In this regard, the AI Act's proposal remains silent.

   At the same time, the research examined the extent to which common standardisation and certification can enhance the protection to the right to privacy and data protection.

Considering common standards and certifications for digital health technologies, the thesis established that currently there is no one single standardisation or certification scheme that can incorporate and ensure compliance with privacy and data protection laws. Thus, a combination of several certification or standardisation schemes should be used to ensure an overall privacy and data protection compliance.

The above-mentioned thesis goals were accompanied by three main research questions:

1. How is big data conceptualised and what is its relationship with digital health technologies and healthcare emergencies?

In this respect, Chapter 3 of the thesis, being the first chapter of the body of the thesis, analysed and discussed the notions of big data, digital health technologies, and healthcare emergencies.

2. To what extent can the current and the proposed EU regulatory initiatives address the balance of the right to privacy, data protection, and the right to health considering digital health technologies?
    a. Considering the specific nature of the Covid-19 pandemic, should the rights to health and the right to privacy be balanced also in sensitive situations such as healthcare emergencies?

Question 2, being the central point of the thesis delved into answering the above questions through an in-depth analysis of the applicable regulatory privacy, data protection, digital health technologies and AI frameworks in the EU and the suggested regulatory proposals at the EU level. Chapters 4, 5, and 6 of the research provide an analysis on the questions.

3. Considering the risk to privacy and data protection in digital health, how can common standardisation and certification of digital health technologies ensure compliance with the applicable privacy and data protection legislation to minimise such risks?

As regards the third question, Chapter 7 offered an answer by delving into a thorough analysis of the regulatory framework surrounding common standardisation and certification schemes in the European Union with a comparative analysis of U.S. regulatory framework, as a competing jurisdiction for digital health technologies. Chapter 7 examined privacy and data protection-related certifications that could be applicable to digital health technologies, analysing the ISO 27000 family standards. It was established that while these standards do not specifically focus on the digital health technologies, these certification standards form a basis for all products and services that aim to ensure privacy and data protection. The research found that the examined ISO frameworks do not provide a guarantee of the GDPR compliance for any technology that processes personal data. Rather it provides a compliance

and assurance mechanism for general privacy compliance, some of which include data protection compliance under the GDPR. The thesis also examined the ISDP 10003 standard, a standard that has been specifically prepared for the GDPR compliance. In this respect, it was observed that such a GDPR-specific standard may be the tool used to ensure and fully implement the GDPR requirements in all products and services processing personal data. At the same time, the ISDP 10003 certification mechanism would fall short on addressing larger risks of cybersecurity of such products of services, which may affect the protection of the right to privacy and data protection. Finally, with regard to health technologies deployed for public health crisis management, we observed that standardisation and certification often play a secondary role in ensuring such technology security, rather than focusing on the privacy or data protection aspects of such technologies.

8.2 Review of Analyses and Findings

To situate the thesis and the research carried within, in Chapter 3 we examined the main concepts related to the research field. In this regard, the thesis analysed the notions of health emergencies, digital health technologies, and big data in the EU privacy and data protection laws, and the ethical/philosophical sides of such notions. The examination considered the absence of single definitions for each of the above-mentioned notions across European legislation. The analyses on the above terms were carried out through a scholarly literature review of articles on the topic and in the context of the applicable regulatory regimes including the GDPR, the WP29 guidelines, and other related legislation. In particular, the thesis discussed key regulations in digital health, privacy, data protection, and health, including:

1. The GDPR;
2. The MDR;
3. The proposed regulation for Artificial Intelligence, the AI Act;
4. Proposed amendments to the NIS directive, and its updated version, the so-called NIS2 Directive;
5. The Cybersecurity Act;
6. Proposal for the Regulation on Serious Cross-Border Threats to Health;
7. Regulation on the Health Technology Assessment; and

8. The proposal for the Common EU Data Space.

The resulting analysis then included a review of the literature on the above-mentioned regulations. The use of these methods in the research revealed that EU law, in the broad sense, does not define either of the notions.

With respect to the term big data, the analysis showcased that, before all else, from the industry standpoint, the value of big data is often seen as a consequence of its analysis and not valuable (or a value) per se, i.e., in its primary, original state. Conversely, when evaluating the notion of big data in terms of EU data protection law, both the GDPR and the CoE take the stance that big data is a value per se, whether attributable to an individual/group or not, thus deserving protection in the digital world. Precisely this discrepancy could be the leading factor in the diverse approach by the big tech companies and privacy scholars bargaining for two different approaches in legislation.

Likewise, digital health technologies both in EU data protection, healthcare, and the international levels are understood as a plethora of various technologies used in the healthcare sector. In this respect the analyses found that the regulatory treatment of digital health technologies highly depends on such technology's specific parameters, scope of use, and target market. For example, in EU legislation we may find several definitions of digital health technologies, varying from medicinal products, medical devices to health technology itself, forming the subject-matter of a particular sectoral legislation.

As observed in Chapter 3, emergency in healthcare is a multi-dimensional notion that, depending on a situation, can involve several different stakeholders, outcomes, and interpretations. This multidimensional nature of a healthcare emergency explains why in the European Union, no single health emergency definition exists either from a legal or from an empirical standpoint. Therefore, this leads to a conclusion that that healthcare emergencies will remain a context-driven notion.

Through a descriptive and exploratory research, Chapter 3 contributed to the literature in the research field, clarifying that certain notions, such as healthcare emergency or digital healthcare technology, are broad concepts that cover a wide range of technologies deployed in healthcare under their umbrella.

On the other hand, the lack of a common definition of the notion of big data is probably what led to misconceptions and misinterpretations of the use of big data in the digital context, especially when considering the data protection landscape.

Chapters 4, 5, and 6 of the body of the thesis analysed and examined the regulatory framework surrounding big data, privacy, data protection, healthcare emergencies, and digital health technologies. The analysis of the regulatory framework carried out led to a handful of conclusions.

First, Chapter 4 established that the dawn of the digital age brought a fundamental shift from the right to privacy to matters of access and control over data, and thus, towards the protection of personal data as evidenced by a historical analysis of privacy and data protection legislation. Such a shift expanded the scope of the rights connected to privacy and individual personality rights which may be threatened by the collection or processing of personal data.

Second, the analyses carried out found that the complex phenomenon of big data as established in Chapter 3 makes it exceptionally challenging to regulate the digital healthcare industry based on big data and AI. The current legislative discipline of big data in the EU reflects the complexity of the phenomenon. This fragmented legislative framework on big data encompasses such fields as fundamental rights, privacy, data protection, cybersecurity, data ethics, data analytics, health informatics, and health law.

This stance revealed that ultimately converging legislative initiatives, developed through the lens of a clear-cut distinction of personal data and non-personal data pursuant to the GDPR, may fall short in tackling the technological changes and effects that big data poses on an individual's life. This is especially evident when various personal data are combined with non-personal data. For example, to allow the identification of individuals due to their behavioural inclinations, where certain personal data of such an individual (such as name or surname) become irrelevant, secondary detail, as a decision may be taken based not on the personal data but on the non-personal secondary data and still carry legal consequences.

Third, Chapter 4 analysed how the provisions contained in the GDPR for personal data protection are transposed into sectorial legislation specifically in the case of digital health technologies. The research was able to establish that the specific regulatory regime applicable to medical devices under the MDR, that also addresses privacy and data protection, does not apply to all digital health technologies. In other words, only digital technologies that satisfy the definition of a medical device under the MDR regime are subject to increased regulatory scrutiny. To exemplify this, the research considered an application that allows individuals to voluntarily trace their sleep quality: it will be required to comply with the GDPR, but would not fall under the MDR regime, since it would not be considered as a medical device in terms of the MDR. Yet, in cases where digital health technologies, such as sensors or remote health

monitoring technologies, which have evolved into legitimate medical devices collecting data concerning health, the GDPR would become a legal co-requisite for the MDR compliance. The research has further observed that the MDR does not establish how compliance with the GDPR for medical devices should be achieved, the MDR simply directs the manufacturers of the medical devices to the GDPR for guidance, as part of its harmonised approach to an overall end-user (consumer) safety and security.

Chapter 5 then continued with the examination of the complex regulatory interplay between European laws on privacy, data protection, and digital health devices deployed in healthcare emergencies. This outlook permitted the research to establish the extent to which the use of big data, which includes personal data, is lawful according to the data protection legislation in healthcare and what limitations, if any, can be drawn in terms of the processing of such data in healthcare emergencies.

The Covid-19 public healthcare emergency was taken as an example for the case study. In this respect, the research established that while the processing of personal, sensitive data, and data concerning health is permitted under the GDPR, the processing of such data not only by governments of the Member States, but also by private organisations, requires a strict set of checks and balances to be maintained in situations of crises.

The thesis examined case studies, focusing on two types of digital health technologies deployed in the Covid-19 pandemic:

1. First-generation pandemic management technologies, namely the exposure notification applications, and
2. Second-generation pandemic management technologies, namely the EU Digital Green Certificate.

The thesis has established that, in terms of privacy and data protection, the deployment of contact-tracing applications in the Covid-19 scenario focused on the general principles of necessity, effectiveness, and proportionality, otherwise known as data-management principles. The proportionality concerning the exposure notification applications entailed that such applications should only have been implemented for two specific purposes: to support the response to the pandemic through the modelling of the spread of the virus, and to notify individuals of their exposure to Covid-19, for instance, via exposure notification. The necessity in terms of the GDPR concerning exposure notification technologies referred to the necessity for the performance of tasks considered to be in the public interest as underlined in Article 6.1(e) of the GDPR. The necessity as established by the Member States and the

European Commission, lay with the necessity of managing and preventing exposure to the Covid-19. The proportionality entailed that such contact tracing applications would only be used during the period of a public healthcare emergency, as established by the governments of the Member States or the EU itself. Finally, it was observed that the adoption of contact-tracing technologies in the EU to contain and combat the epidemiological emergency of the Covid-19 in a highly complex context was an unprecedented challenge for the Member States' governments.

Regarding proofs of vaccination, the thesis established that a comprehensive regulatory regime and guidance was required for the introduction of such proofs of vaccination, not only in terms of data protection, but also as regards ethical considerations for such technologies. While the EU has issued such guidance, the guidance failed to address some of the data protection and ethics concerns to a full extent, especially those relating to the sharing of data between the authorities of the Member States. The research also established that the vaccination certificates do not necessarily violate equal treatment as the obtainment of such passports is not based on factors such as religion or race, but rather on hard scientific evidence. Indeed, even the ECtHR has been made to decide on the proof of vaccination measures adopted by the French government on two separate occasions: two separate individual applications tried to argue that the deployed requirements to provide proofs of vaccinations infringed individual rights enshrined in the ECHR. In both cases the ECtHR found the cases inadmissible due to the lack of testimony that individual rights were infringed.

Chapter 5 also identified and addressed several shortcomings of the existing regulatory framework concerning healthcare emergencies at the Union level. The legislative proposal for the Regulation on Serious Cross-Border Threats to Health can be described as a building block for the Union's public health crisis management system, as it would allow the Union to address new healthcare threats more rapidly to provide a coordinated response. The proposed regulation complemented several already existing EU measures in the field of crisis management, including the creation of the European health data space which would facilitate research and innovation based on real-world data and ensure epidemiological preparedness. The proposed regulation thus touched upon data protection aspects as regards to the sharing of data and the development of and EU-wide infrastructure for epidemiological surveillance. However, the said proposal did not examine what impact such establishment would have on the right to privacy and personal data. The proposed regulation provided the right and power "to formally recognise a public health emergency" at the Union level. Such health

emergencies may include pandemics and other health threats that affect health at the Union level. The right to recognise a state of emergency at the Union level is aimed at facilitating better public health crisis management at the Union level, by streamlining national procedures throughout the EU, leaving the Member States with ample space to impose further national rules and procedures for public health crisis management.

Chapter 6 of the body of the thesis focused on the importance of the current European policy and legislative proposals around digital health technologies, from the perspective of the right to data protection and the right to privacy. Based on the premise that ensuring the right to privacy and data protection in digital health technologies can be achieved through legislative means, the chapter analysed three key European initiatives:

1. the policy proposal the European Health Union;
2. the proposed regulation on the Common EU Health Data Space; and finally,
3. the proposal for the regulation for Artificial Intelligence.

Considering the European Health Union, the thesis observed that, rather than establishing a true health union which focuses on facilitating equal health standards among Member States' health systems, the proposal's content does not live up to the proposal's name. Rather, the proposal in essence updates the currently existing EU health crises governance system, by extending powers to the ECDC to collect and process health-related data to predict and prepare for future Europe-wide public health crises. In this respect, the Covid-19 pandemic can be considered a "favourable contextual condition"[533] that facilitated the quick update of the currently existing rules on public health crisis management at the EU level.

Consequently, the envisaged European Health Union comes as a politically planned response to manage the public's disappointment regarding the Union's limited ability to respond to the Covid-19 pandemic, even with the crisis management mechanisms that were available.

As regards the EU Health Data Space, ensuring the fundamental rights to data protection and privacy will remain a battle. Even if the right to privacy and data protection are not absolute rights and may be limited, any limitations would, however, require a careful analysis, being the "bread and butter" of the CJEU. Therefore, in terms of the proposal for the EU Health Data Space, it will remain fundamental to establish detailed data management plans and policies, which would need to take a primary role to ensure legal access and processing of citizen personal data, in line with the GDPR. Additionally, the data governance mechanisms

[533] Bazzan (n 369).

will take a prominent role in assuring a lawful, transparent, and ethical management of the data involved, including accountability mechanisms in the EU Health Data Space in cases where there are fundamental rights' implications. Finally, the sharing of data through the EU Health Data Space may become an instrument allowing for the better preparedness of future health-related crises.

In the final section of Chapter 6, the researcher addressed the proposal for the regulation of Artificial Intelligence, a horizontal regulation laying down general rules for the use of AI. The legal analysis of the proposal indicated that the AI Act proposal is a strategically targeted regulation considering the envisaged growth of the AI system's market. The AI Act proposal includes novel governance and enforcement mechanisms on fundamental rights and applicable safety requirements. Also, the proposal attempts to be the cornerstone legislation in ensuring legal certainty in AI. It was observed that, irrespective of the goals it aims to achieve, the AI Act stresses the boundaries of non-hindrance of technological innovation due to regulatory overlaps with the existing regulations, creating regulatory ambiguities, that are particularly apparent in the case of medical devices. In practice, this will translate into additional regulatory and technical requirements that would need to be transposed by the developers of the AI when deploying an AI-based digital health technology, including requirements such as transparency, decision making, or human oversight that ought to be addressed under the AI Act proposal.

Also, the AI Act proposal raises questions as to whether AI providers will ultimately fail to recognise the status of individuals adversely affected by the AI, including the lack of some of the procedural rights, such as the right to seek redress or lack of a compliance mechanism, considering AI manufacturers' competing interests vis-à-vis users of the same AI technologies[534]. Similar criticism has led researchers to conclude that "big tech emerges virtually unscathed under the new AI legislation, despite being the object of widespread and growing concern"[535]. Apart from several drawbacks of the AI Act proposal, the AI Act proposal will provide clarity on the boundaries of permissible use of AI technologies, including digital health technologies, based on risk. Such a risk-based mechanism would facilitate safer technology deployment for AI systems that are high-risk and may affect the safety and security of users, such as healthcare devices. The proposal also calls on the Member States to support AI regulation and innovation via regulatory testing, through

[534] Smuha and others (n 423).
[535] ibid.

regulatory sandboxes or via policy prototyping, which ought to further facilitate innovation in the EU.

Steering away from regulation of big data, privacy, and data protection, Chapter 7 of the thesis presented a discussion on the role of cybersecurity in digital health technologies. Focus was placed on private standards and certification schemes that would enable greater privacy and data protection in digital health technologies. The discussion in Chapter 7 started with an analysis of the European legislative framework regarding the applicability of cybersecurity measures that further consolidate personal data protection and privacy in Europe, through the establishment and use of common technical standards and certifications for digital health technologies. In this respect, Chapter 7 highlighted the broad material scope of the EU privacy law, pointing out that privacy laws do not only cover the GDPR but also encompass supporting sectorial legislation such as the EU Cybersecurity Act, and the NIS2 directive.

Drawing a parallel with a competing jurisdiction in cybersecurity and standardisation, the U.S., the research demonstrated how different regulatory approaches impact innovation and research in digital health technologies. The analysis of the above-mentioned legislative frameworks led to a first conclusion that there is a multi-layered relationship between ensuring data privacy in digital health technologies. Ensuring privacy and data protection is achieved via the establishment of an EU-wide legislative framework, i.e., the EU's Cybersecurity Act, and through supporting technical guidelines, standards, and certifications. When assessed altogether, all these mechanisms ensure that risks associated with the right to privacy and data protection are addressed by the developers of technologies.

The chapter then examined the applicability of specific standards, namely the ISO 27000 family standards that ensure IT and data security, and GDPR specific standards, namely the ISDP 10003 standards to digital health technologies. The analysis stems from the result of a 6-months internship at a company in Turin, Italy which is developing a data management system to be used by and between a hospital, patients, and the University of Turin. The aim of such a data management system is three-fold: 1. it will facilitate quicker access to patient data for the medical personnel treating the patient; 2. it will facilitate health research at a national level; 3. It will provide more patient-centred healthcare.

In this regard, it was observed that the applicability of third-party standards and certification schemes throughout the development stages of the project allows privacy and data protection within the developed technology to be greatly increased. The research also observed that currently no single standard exists that can comprehensively ensure both privacy and the GDPR norms. Thus, the application of both ISO 27000 family standards and of the GDPR

specific standards, such as ISDP 10003, is suggested to ensure privacy and personal data protection within digital health technologies.

8.3 Final Observations and Possible Future Research Directions

The multifaceted nature of this research project argued that ensuring the right to privacy and personal data in certain scenarios, such as healthcare emergencies, the introduction and deployment of digital health technologies, may hinder the right to data protection and privacy. Such hindering of the right to privacy and the right to data protection, especially in healthcare emergencies, may lead to a slower adoption of technological solutions in healthcare. Nonetheless, the possible impacts on privacy and data protection in healthcare emergencies, that range from unauthorised surveillance and other various GDPR violations, common standards and certification schemes, may be used as tools to enhance privacy and data protection in digital health technologies. Ensuring that such rights are protected remains an ongoing, case-by-case based exercise in digital health technologies based on big data or AI.

It is unmistakable that the European privacy and data protection regime's benefits on the individual rights to privacy and data protection are vast and able to protect our fundamental rights even in sensitive healthcare emergency scenarios, where rapid response is essential. The said regimes stretch to affect and touch upon a wide variety of legal domains where digital health technologies are concerned. Therefore, the future work that follows from the research conducted in this thesis gives opportunities for forthcoming work to turn several different directions. One direction for the research would be to further explore the medical devices' industry and the regulatory impact of proposed AI regulation to medical devices in EU, especially focusing on technologies deployed in time-sensitive situations such as healthcare emergencies. This thesis also lays the ground for possible further exploration and research in the applicability and the relationship between the regulatory frameworks for AI and digital health technologies for health emergencies' research and innovation.

9 Bibliography

Legislative Documents, Guidelines, and Opinions

Art. 29 WP, ‘Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is “Likely to Result in a High Risk” for the Purposes of Regulation 2016/679’ (2017) WP 248 rev Article 29 Working Party 22

Article 29 Data Protection Working Party, ‘Opinion 03/2013 on Purpose Limitation’ (2013)

Constitution of the Republic of Lithuania (Adopted by Citizens of the Republic of Lithuania in the Referendum of 25 October 1992)

Council of Europe, CC of C 108, ‘Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data’ (2017)

EDPB, ‘EDPB-EDPS Joint Opinion 03 / 2022 on the Proposal for a Regulation on the European Health Data Space Adopted on 12 July 2022’ 1

EDPB and EDPS, ‘EDPB-EDPS Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)’

EDPS, ‘Opinion 3/2020 on the European Strategy for Data’ (2020)

ENISA, Good Practices for Security of Internet of Things in the Context of Smart Manufacturing (2018)

The EU Charter of Fundamental Rights

The European Convention on Human Rights

European Court of Human Rights, ‘Guide on Article 15 of the European Convention on Human Rights Derogation in Time of Emergency’

European Data Protection Board, ‘Guidelines 03/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the COVID-19 Outbreak’ (2020)

European Data Protection Board, ‘Guidelines 04/2020 on the Use of Location Data and

Contact Tracing Tools in the Context of the COVID-19 Outbreak' (2020)

Medical Device Coordination Group, 'Guidance on Cybersecurity for Medical Devices' [2019] MDCG 2019-16 Rev.1

Guidance on Cybersecurity in Medical Devices - Artical 103 of Regulation (EU)2017/745' [2019] Medical Device 1

European Data Protection Supervisor. Preliminary Opinion 8/2020 on the European Health Data Space

Supervisor EDPB, 'Opinion 3/2020 in the European Strategy for Data' (2020)

The European Commission, 'Health Technology Assessment Regulation'

MDCG, 2021-05 Guidance on Standartisation for Medical Devices.Pdf' (2021)

The European Data Strategy

Universal Declaration of Human Rights

Working Party 29, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679,'(2017)

Case C-613/14, Judgment of the Court (Fourth Chamber) of 5 March 2015 Boston Scientific Medizintechnik GmbH v AOK Sachsen-Anhalt Requests for a preliminary ruling from the Bundesgerichtshof

Case,C-329/16.Judgment of the Court (Fourth Chamber) of 7 December 2017 Syndicat national de l'industrie des technologies médicales (Snitem) and Philips France v Premier ministre and Ministre des Affaires sociales et de la Santé. Request for a preliminary ruling from the Conseil d'État (France) (2017)

Von Hannover v Germany (no 2) [GC] - 40660/08 and 60641/08 Judgment 722012 [GC]

Le Mailloux v. France, HUDOC - European Court of Human Rights <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:[%22003-6873639-9217565%22]%7D>

EU Commission, Proposal for a Regulation of the European Parliament and of the Council laying dow harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts COM/2021/206 final 2021

European Commission, Proposal for a Regulation of the European Parliament and the Council on serious cross-border threats to health and repealing Decision No 1082/2013/EU 2020

Regulation (EU) 2021/2282 of the European Parliament and of the Council of 15 December 2021 on health technology assessment and amending Directive 2011/24/EU (Text with EEA relevance) PE/80/2021/INIT 2021 1

Proposal for a Regulation on the European Health Data Space (Text with EEA relevance) 2022
European Parliament, Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use 2001

European Parliament OL 88, Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare 2011 45

Il Presidente Della Repubblica, Decreto Legge 30 Aprile 2020, n.28 2020

OJ L 117, Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance.) 2017,176

OJ L 151, Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) 2018,15

Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic 2021,1

The European Commission, Annexes to the Proposal for a Regulation of the European Parliament and of the Council Laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts 2021

The European Parliament, Proposal for a Regulation of the European Parliament and of the Council laying dow harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts COM/2021/206 final 2021

The European Parliament and The Council, Regulation (EU) 2016/679 of the European Parliament and 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 2016

The European Parliament OL 201, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) 2002 37

WHO, Resolution on Health Technologies 2015

Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC 2013 (OJ L 293) 1

International Health Regulations (2005) 2005 (Lancet) 1249

OHCHR, International Covenant on Civil and Political Rights

Proposal for a Reglation of the European Parliament and the Council on the European Health Data Space COM(2022) 197 final 2022 (European Commission) 1

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/ 2017

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EE 2017

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.) 2018 (OJ L 303, 28112018, p 59–68

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) 2019 15

Literature

Aho B and Duffield R, ‘Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China’ (2020) 49 https://doi-org.proxy.bnl.lu/10.1080/03085147.2019.1690275 187 <https://www-tandfonline-com.proxy.bnl.lu/doi/abs/10.1080/03085147.2019.1690275>

Albrecht UV, Hillebrand U and von Jan U, ‘Relevance of Trust Marks and CE Labels in German-Language Store Descriptions of Health Apps: Analysis’ (2018) 6 JMIR mHealth and uHealth </pmc/articles/PMC5943626/>

Alemanno A, ‘The European Response to CoviD-19: From Regulatory Emulation to Regulatory Coordination?’ (2020) 11 European Journal of Risk Regulation 307 <https://doi.org/10.1017/err.2020.44>

‘Towards a European Health Union: Time to Level Up’ (2020) 11 European Journal of Risk Regulation 721 <https://doi.org/10.1017/err.2020.106>

Anderson S and Williams T, ‘Cybersecurity and Medical Devices: Are the ISO/IEC 80001-2-2 Technical Controls up to the Challenge?’ (2018) 56 Computer Standards & Interfaces 134
Andreu-Perez J and others, ‘Big Data for Health’ (2015) 19 IEEE Journal of Biomedical and Health Informatics 1193

Anr / and others, ‘Personal and Non-Personal Data in the Context of Big Data’ (2017)

‘Are Wearables Medical Devices Requiring a CE-Mark in the EU? | Covington Digital Health’ <https://www.covingtondigitalhealth.com/2019/01/are-wearables-medical-devices-requiring-a-ce-mark-in-the-eu/>

Aringhieri R and others, ‘Emergency Medical Services and beyond: Addressing New Challenges through a Wide Literature Review’ (2017) 78 Computers & Operations Research 349 <https://www.sciencedirect.com/science/article/pii/S0305054816302362>

Aringhieri R and others, ‘Evaluating the Dispatching Policies for a Regional Network of Emergency Departments Exploiting Health Care Big Data’ (Springer, Cham 2018) <http://link.springer.com/10.1007/978-3-319-72926-8_46>

Attarian R and Hashemi S, ‘An Anonymity Communication Protocol for Security and Privacy of Clients in IoT-Based Mobile Health Transactions’ (2021) 190 Computer Networks 107976

Bazzan G, ‘Exploring Integration Trajectories for a European Health Union’ (2020) 11 European Journal of Risk Regulation 736

Beaussier AL and Cabane L, ‘Strengthening the EU’s Response Capacity to Health Emergencies: Insights from EU Crisis Management Mechanisms’ (2020) 11 European Journal of Risk Regulation 808 <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/strengthening-the-eus-response-capacity-to-health-emergencies-insights-from-eu-crisis-management-mechanisms/A8DCBA29DCC1985BB0CDAB50AEC38127>

Benjamin AH and others, ‘Legal Policy & Pandemics’ (2021) 1 The Journal of the Global Pandemic Network

Beqiraj J and others, ‘IEAI White Paper "Rule of Law, Legitimacy and Effective COVID-19 Control Technologies” Institute for Ethics in Artificial Intelligence’ [2022] EAI White Paper Series <https://www.ieai.sot.tum.de/ieai-white-paper-series-rule-of-law/>

Berendt B, ‘AI for the Common Good?! Pitfalls, Challenges, and Ethics Pen-Testing’ (2019) 10 Paladyn, Journal of Behavioral Robotics 44 <https://www.degruyter.com/document/doi/10.1515/pjbr-2019-0004/html>

Biasin E and Kamenjašević E, ‘Cybersecurity of Medical Devices: New Challenges Arising from the AI Act and NIS 2 Directive Proposals’ (2022) 3 International Cybersecurity Law Review 2022, Vol. 3, Pages 163-180 163 <https://www.scilit.net/article/f6fc072a0aa5803281f2e8f6da408f16>

Boyd D and Crawford K, ‘Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon’ (2012) 15 https://doi-org.proxy.bnl.lu/10.1080/1369118X.2012.678878 662 <https://www-tandfonline-com.proxy.bnl.lu/doi/abs/10.1080/1369118X.2012.678878>

Brewczynska M, ‘The Polish Government’s Actions to Fight Covid-19: A Critical Look at the “Selfie App” and Direct Access to Location Data’ (2020) 6 European Data Protection

Law Review (EDPL)
<https://heinonline.org/HOL/Page?handle=hein.journals/edpl6&id=314&div=&collection=>

Brewczyńska M, 'Contact Tracing Apps in Poland A New World for Data Privacy', vol 2 (2020)

Brewczyńska, Magdalena. European Data Protection Law Review (EDPL): Contact Tracing Apps in Poland A New World for Data Privacy, vol 2(2020)

'Poland: The Polish Government's Actions to Fight COVID-19: A Critical Look at the "Selfie App" and Direct Access to Location Data' (2020) 6 European Data Protection Law Review 301

Bu-Pasha S, 'The Controller's Role in Determining "High Risk" and Data Protection Impact Assessment (DPIA) in Developing Digital Smart City' [2020] https://doi.org/10.1080/13600834.2020.1790092

Cao HR and Zhan C, 'A Novel Emergency Healthcare System for Elderly Community in Outdoor Environment' (2018) 2018 Wireless Communications and Mobile Computing

Cartledge C, 'How Many Vs Are There in Big Data?' 1 http://www.clc-ent.com/TBDE/Docs/vs.pdf

Casanovas P and others, 'Regulation of Big Data: Perspectives on Strategy, Policy, Law and Privacy' (2017) 7 Health and Technology 2017 7:4 335
<https://link.springer.com/article/10.1007/s12553-017-0190-6>

Cohen IG and others (eds), 'The Future of Medical Device Regulation: Innovation and Protection' <https://www.cambridge.org/core/books/future-of-medical-device-regulation/7ABD9575718C5F31B69E4CE00DD7F7E7>

Colombo F, Oderkirk J and Slawomirski L, 'Health Information Systems, Electronic Medical Records, and Big Data in Global Healthcare: Progress and Challenges in OECD Countries' [2020] Handbook of Global Health 1

Contardi M, 'Changes in the Medical Device's Regulatory Framework and Its Impact on the Medical Device's Industry: From the Medical Device Directives to the Medical Device Regulations' (2019) 12 Erasmus Law Review 166

Cox M and Ellsworth D, 'Application-Controlled Demand Paging for out-of-Core Visualization' [1997] Proceedings of the IEEE Visualization Conference 235
Custers B and others, 'Lists of Ethical, Legal, Societal and Economic Issues of Big Data Technologies' [2018] SSRN Electronic Journal 1

David A. Frenkel* and David M. Wood, 'Patients' rights to privacy and public interest'(2015) 34 Medicine and Law 85

Delacroix S and Lawrence ND, 'Do Property Rights in Personal Data Make Sense after the Big Data Turn?: Individual Control and Transparency' (2017) 9 International Data Privacy Law 236 <https://papers.ssrn.com/abstract=3070228>

Din S and Paul A, ‘Erratum to “Smart Health Monitoring and Management System: Toward Autonomous Wearable Sensing for Internet of Things Using Big Data Analytics [Future Gener. Comput. Syst. 91 (2019) 611–619]” (Future Generation Computer Systems (2019) 91 (611–619), (S01677’ 1350)

Dion M, AbdelMalik P and Mawudeku A, ‘Big Data and the Global Public Health Intelligence Network (GPHIN)’ (2015) 41 Canada Communicable Disease Report 209

Eberle EJ, ‘The Methodology of Comparative Law’ (2011) 16 Roger Williams University Law Review<https://heinonline.org/HOL/Page?handle=hein.journals/rwulr16&id=53&div=5&collection=journals>

Ebers M, ‘Standardizing AI - The Case of the European Commission’s Proposal for an Artificial Intelligence Act’ [2021] SSRN Electronic Journal <https://papers.ssrn.com/abstract=3900378>

Ellul J and others, ‘A Pragmatic Approach to Regulating Artificial Intelligence: A Technology Regulator’s Perspective’ <http://arxiv.org/abs/2105.06267>

Erikson SL, ‘Cell Phones ≠ Self and Other Problems with Big Data Detection and Containment during Epidemics’ (2018) 32 Medical Anthropology Quarterly 315 </pmc/articles/PMC6175342/?report=abstract>

Evans D, ‘The Internet of Everything How More Relevant and Valuable Connections Will Change the World’ (2015)

Fiazza M, ‘The EU Proposal for Regulating AI : Foreseeable Impact on Medical Robotics’ (2022)

Finck M and Pallas F, ‘They Who Must Not Be Identified - Distinguishing Personal from Non-Personal Data Under the GDPR’ [2019] SSRN Electronic Journal <https://papers.ssrn.com/abstract=3462948>

Floridi L, ‘The Method of Levels of Abstraction’ (2008) 18 Minds and Machines 303
‘The European Legislation on AI: A Brief Analysis of Its Philosophical Approach’ (2021) 34 Philosophy & Technology 215 <https://link.springer.com/10.1007/s13347-021-00460-9>

AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations’ (2018) 28 Minds and Machines 689 <https://link.springer.com/article/10.1007/s11023-018-9482-5>

Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies’ (2021) Internet Policy Review:Journal on Internet Regulation 1 https://policyreview.info/articles/analysis/safeguarding-european-values-digital-sovereignty-analysis-statements-and-policies

Conformity Assessments and Post-Market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation’ (2021) Minds and Machines 1

<https://link.springer.com/article/10.1007/s11023-021-09577-4>

Floridi L and Taddeo M, 'What Is Data Ethics?' (2016) 374 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20160360 <https://royalsocietypublishing.org/doi/10.1098/rsta.2016.0360>

Forgó N, Hänold S and Schütze B, 'The Principle of Purpose Limitation and Big Data' [2017] Perspectives in Law, Business and Innovation 17 <https://link.springer.com/chapter/10.1007/978-981-10-5038-1_2>

Fuster GG and Jasmontaite L, 'Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights' (2020)

Gabel A and others, 'MHealth Applications for Goal Management Training - Privacy Engineering in Neuropsychological Studies' (2018) 526 IFIP Advances in Information and Communication Technology 330

Gasser U and others, 'Digital Tools against COVID-19: Taxonomy, Ethical Challenges, and Navigation Aid' (2020) 2 The Lancet Digital Health e425 <www.thelancet.com/digital-health>

Gerybaite A, 'Digital Governance: The Case of Proofs of Vaccination' (2021) ACM International Conference Proceeding Series 450

Gerybaite A and Aurucci P, 'Big Data and Pandemics: How to Strike in the Age of GDPR' (2020) Intelligent Environments 2020: Workshop Proceedings of the 16th International Conference on Intelligent Environments 115

Gloria González Fuster AS, 'Big Data and Smart Devices and Their Impact on Privacy' [2015] European Parliament, Study of the LIBE Committee

Goffredo R, Accoto D and Guglielmelli E, 'Swallowable Smart Pills for Local Drug Delivery: Present Status and Future Perspectives' (2015) 12 http://dx.doi.org.proxy.bnl.lu/10.1586/17434440.2015.1061933 585 <https://www-tandfonline-com.proxy.bnl.lu/doi/abs/10.1586/17434440.2015.1061933>

Gotz D and Borland D, 'Data-Driven Healthcare: Challenges and Opportunities for Interactive Visualization' (2016) 36 IEEE Computer Graphics and Applications

Günther WA and others, 'Debating Big Data: A Literature Review on Realizing Value from Big Data' (2017) 26 Journal of Strategic Information Systems 191

Ienca M and Vayena E, 'On the Responsible Use of Digital Data to Tackle the COVID-19 Pandemic' (2020) 26 Nature Medicine 463 <https://doi.org/10.1038/s41591-020-0832-5>

Jaquet-Chiffelle DO and Loi M, 'Ethical and Unethical Hacking' (2020) 21 International Library of Ethics, Law and Technology 179 <https://serval.unil.ch/notice/serval:BIB_CB652A6CE0EC>

Jarman H, Rozenblum S and Huang TJ, 'Neither Protective nor Harmonised: The

Crossborder Regulation of Medical Devices in the EU' [2020] Health Economics, Policy and Law 51

Jayaprakash N and others, 'Crowding and Delivery of Healthcare in Emergency Departments: The European Perspective.' (2009) 10 The western journal of emergency medicine 233 <http://www.ncbi.nlm.nih.gov/pubmed/20046239>

Jenny Bergholm, 'EDPB-EDPS Opinion: Four Lessons for the AI Regulation and Data Protection - CITIP Blog' (2021) <https://www.law.kuleuven.be/citip/blog/edpb-edps-opinion-four-lessons-for-the-ai-regulation-and-data-protection/>

John Rawls (Stanford Encyclopedia of Philosophy)' <https://plato.stanford.edu/entries/rawls/>

Kahnbach L and others, 'Quality and Adoption of COVID-19 Tracing Apps and Recommendations for Development: Systematic Interdisciplinary Review of European Apps' (2021) 23 J Med Internet Res 2021;23(6):e27989 https://www.jmir.org/2021/6/e27989 e27989 <https://www.jmir.org/2021/6/e27989>

Kamara I, 'Co-Regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation "Mandate"' (2017) 8 European Journal of Law and Technology <https://www.ejlt.org/index.php/ejlt/article/view/545/723>

Kitchin R, The Data Revolution : Big Data, Open Data, Data Infrastructures & Their Consequences

Klessova S and others, 'ICT Policy, Research, and Innovation: Perspectives and Prospects for EU-US Collaboration' [2020] ICT Policy, Research, and Innovation: Perspectives and Prospects for EU-US Collaboration 1<https://onlinelibrary.wiley.com/doi/book/10.1002/9781119632481>

Klugman CM and others, 'The Ethics of Smart Pills and Self-Acting Devices: Autonomy, Truth-Telling, and Trust at the Dawn of Digital Medicine' (2018) 18 https://doi-org.proxy.bnl.lu/10.1080/15265161.2018.1498933

Kolfshooten Van H., 'EU Coordination of Serious Cross-Border Threats to Health: The Implications for Protection of Informed Consent in National Pandemic Policies' (2019) 10 European Journal of Risk Regulation 635 <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/eu-coordination-of-serious-crossborder-threats-to-health-the-implications-for-protection-of-informed-consent-in-national-pandemic-policies/91117A9FE70273CCCD00F3203719BD98>

Koolen C, 'Transparency and Consent in Data-Driven Smart Environments' [2020] SSRN Electronic Journal <https://papers.ssrn.com/abstract=3597736>

Lachaud E, 'ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification' (2020) 6 European Data Protection Law Review 194

Laney, D. (2001) 3D Data Management Controlling Data Volume, Velocity and Variety.

META Group Research Note, 6. - References - Scientific Research Publishing' <https://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/ReferencesPapers.aspx?ReferenceID=1611280>

Levallois-Barth C and Zylberberg H, 'A Purpose-Based Taxonomy for Better Governance of Personal Data in the Internet of Things Era: The Example of Wellness Data' 139
Lindskou TA and others, 'The Danish Prehospital Emergency Healthcare System and Research Possibilities'

Liveri D, Sarri A and Skouloudi C, Security and Resilience in EHealth (2015) https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/ehealth_sec/security-and-resilience-in-ehealth-infrastructures-and-services

Lobmayr B, 'An Assessment of the EU Approach to Medical Device Regulation against the Backdrop of the US System' (2010) 1 European Journal of Risk Regulation 137 <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/abs/an-assessment-of-the-eu-approach-to-medical-device-regulation-against-the-backdrop-of-the-us-system/2080FE575590A8DCB51DB513AEF75BCA>

Lundstedt L, 'International Jurisdiction over Crossborder Private Enforcement Actions under the GDPR' [2018] SSRN Electronic Journal <https://papers.ssrn.com/abstract=3159854>

Maccarthy M and Propp K, 'Machines Learn That Brussels Writes the Rules: The EU's New AI Regulation' [2021] Brookings.Edu 4 https://www.brookings.edu/blog/techtank/2021/05/04/machines-learn-that-brussels-writes-the-rules-the-eus-new-ai-regulation/

Maccioni G and Giansanti D, 'Medical Apps and the Gray Zone in the Covid-19 Era: Between Evidence and New Needs for Cybersecurity Expansion' (2021) 9 Healthcare (Switzerland) 430 <https://www.mdpi.com/2227-9032/9/4/430/htm>

Majumder S and others, 'Smart Homes for Elderly Healthcare—Recent Advances and Research Challenges' (2017) 17 Sensors (Basel)

Making AD, 'Global Attitudes AI , Machine Surveillance as Towards a Service Learning & Automated Decision Making The European AI-Assisted Mass Surveillance Marketplace Surveillance as a Service'

Mantelero A, 'Regulating Big Data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework' (2017) 33 Computer Law and Security Review 584

Mantelero A and Vaciago G, 'Data Protection in a Big Data Society. Ideas for a Future Regulation' (2015) 15 Digital Investigation 104

Matus KJM and Veale M, 'Certification Systems for Machine Learning: Lessons from Sustainability' [2021] Regulation & Governance <https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12417>

Meszaros J, Compagnucci MC and Minssen T, 'The Interaction of the Medical Device Regulation and the GDPR : Do European Rules on Privacy and Scientific Research Impair the Safety & Performance of AI Medical Devices ? II . Collection and Processing of Health Data under the GDPR Modern Healthcare Sys' (2020) 3501545 1

Micozzi FP, 'Le Tecnologie, La Protezione Dei Dati e l'emergenza Coronavirus: Rapporto Tra Il Possibile e Il Legalmente Consentito' (2020) 2 BioLaw Journal 1

Minssen T and others, 'The EU-US Privacy Shield Regime for Cross- Border Transfers of Personal Data under the GDPR: What Are the Legal Challenges and How Might These Affect Cloudbased Technologies, Big Data, and AI in the Medical Sector?' <https://papers.ssrn.com/abstract=3651094>

Minssen T, Mimler M and Mak V, 'When Does Stand-Alone Software Qualify as a Medical Device in the European Union? — The Cjeu's Decision in Snitem and What It Implies for the next Generation of Medical Devices' (2020) 28 Medical Law Review 615 <https://academic.oup.com/medlaw/article/28/3/615/5865470>

Mökander J and Floridi L, 'Ethics-Based Auditing to Develop Trustworthy AI' (2021) 31 Minds and Machines 323 <https://link.springer.com/article/10.1007/s11023-021-09557-8>

Mooney SJ and Pejaver V, 'Big Data in Public Health: Terminology, Machine Learning, and Privacy' (2018) 39 Annual Review of Public Health 95

Morley J and others, 'The Debate on the Ethics of AI in Health Care: A Reconstruction and Critical Review' 1 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3486518#references-widget

Morley J, Floridi L and Goldacre B, 'The Poor Performance of Apps Assessing Skin Cancer Risk' (2020) 368 BMJ m428 <http://www.bmj.com/lookup/doi/10.1136/bmj.m428>

Mulder T, 'The Role of Law in Protecting Personal Data Generated by Health Apps and Wearables' (University of Groningen 2022)

Narayanan A and Shmatikov V, 'Robust De-Anonymization of Large Sparse Datasets'

Orlando D, 'If Science Fiction Inspires the Law: Recent Examples with the EU Proposal for an AI Regulation' (2021) <https://limo.libis.be/primo-explore/fulldisplay?docid=LIRIAS3463286&context=L&vid=Lirias&search_scope=Lirias&tab=default_tab&lang=en_US&fromSitemap=1>

Orucu E, 'Methodological Aspects of Comparative Law' (2006) 8 European Journal of Law Reform<https://heinonline.org/HOL/Page?handle=hein.journals/ejlr8&id=37&div=10&collection=journals>

Pagallo U, 'The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection' (2017) 3 European Data Protection Law Review (EDPL) 34 <https://iris.unito.it/handle/2318/1640445>

Pagallo U, 'Sovereigns, Viruses, and the Law: The Normative Challenges of Pandemic in

Today's Information Societies' [2020] SSRN Electronic Journal

Pagallo U, 'The Collective Dimensions of Privacy in the Information Era: A Comparative Law Approach' (2020) XI Annuario di diritto comparato e di studi legislativi 115

Pagallo U, 'Sovereigns, Viruses, and the Law: The Normative Challenges of Pandemic in Today's Information Societies' [2020] SSRN Electronic Journal <https://papers.ssrn.com/abstract=3600038>

Pagallo U, Casanovas P and Madelin R, 'The Middle-out Approach: Assessing Models of Legal Governance in Data Protection, Artificial Intelligence, and the Web of Data' (2019) 7 Theory and Practice of Legislation 1

Pagallo U, Durante M and Monteleone S, 'What Is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT' 59

Palmirani M, 'Big Data and Knowledge' (2020) IX Rivista di filosofia del diritto 73 <https://www.rivisteweb.it/doi/10.4477/97021>

Pupillo L, EU Cybersecurity and the Paradox of Progress (2018) https://ssrn.com/abstract=3131559No2018/06,

Purtova N, 'The Law of Everything. Broad Concept of Personal Data and Overstretched Scope of EU Data Protection Law' [2017] SSRN Electronic Journal

EHealth Spare Parts as a Service: Modular EHealth Solutions and Medical Device Reform' (2017) 24 European Journal of Health Law 463 <http://catalogue.fi-star.eu/>

Quinn P, 'The EU Commission's Risky Choice for a Non-Risk Based Strategy on Assessment of Medical Devices' (2017) 33 Computer Law and Security Review 361 <http://dx.doi.org/10.1016/j.clsr.2017.03.0190267-3649/www.sciencedirect.com>

The EU Commission's Risky Choice for a Non-Risk Based Strategy on Assessment of Medical Devices' (2017) 33 Computer Law and Security Review 361

Rathore MM and others, 'Real-Time Medical Emergency Response System: Exploiting IoT and Big Data for Public Health' (2016) 40 Journal of Medical Systems 283 <http://link.springer.com/10.1007/s10916-016-0647-6>

Rocher L, Hendrickx JM and de Montjoye YA, 'Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models' (2019) 10 Nature Communications 1 <https://doi.org/10.1038/s41467-019-10933-3>

Rothstein MA, 'Is Deidentification Sufficient to Protect Health Privacy in Research?' (2010) 10 The American Journal of Bioethics 3 <http://www.tandfonline.com/doi/abs/10.1080/15265161.2010.494215>

Rozek LS and others, 'Understanding Vaccine Hesitancy in the Context of COVID-19: The Role of Trust and Confidence in a Seventeen-Country Survey' (2021) 66 International Journal of Public Health

Ruck A, ‘Information and Stakeholders’ Day on Smart Wearables Report’ (2015) <http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDo>

Rumbold JMM and Pierscionek BK, ‘A Critique of the Regulation of Data Science in Healthcare Research in the European Union’ (2017) 18 BMC Medical Ethics 27 <http://bmcmedethics.biomedcentral.com/articles/10.1186/s12910-017-0184-y>

Salerno J and others, ‘Untangling the Ethical Intersection of Epidemiology, Human Subjects Research, and Public Health’ (2019) 34 Annals of Epidemiology 1

Scherer MU, ‘Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies’ (2015) 29 Harvard Journal of Law & Technology <https://heinonline.org/HOL/Page?handle=hein.journals/hjlt29&id=365&div=15&collection=journals>

Scheuer C and others, ‘European Integration through Standardisation: How Judicial Review Is Breaking down the Club House of Private Standardisation Bodies’ (2013) 50 Common Market Law Review 145 <https://research.tilburguniversity.edu/en/publications/european-integration-through-standardisation-how-judicial-review->

Schneider G, ‘Health Data Pools under European Policy and Data Protection Law: Research as a New Efficiency Defence?’ (2020) <https://www.rand.org/pubs/>

Schrama W, ‘How to Carry out Interdisciplinary Legal Research. Some Experiences with an Interdisciplinary Research Method’ (2011) 7 Utrecht Law Review 147

Shadmi E and others, ‘Predicting 30-Day Readmissions with Preadmission Electronic Health Record Data’ (2015) 53 Medical care 283 <https://pubmed.ncbi.nlm.nih.gov/25634089/>

Shameer K and others, ‘Translational Bioinformatics in the Era of Real-Time Biomedical, Health Care and Wellness Data Streams’ (2017) 18 Briefings in Bioinformatics 105 <https://academic.oup.com/bib/article-lookup/doi/10.1093/bib/bbv118>

Sheppard MK, ‘MHealth Apps: Disruptive Innovation, Regulation, and Trust — A Need for Balance’ (2020) 28 Medical Law Review 549

Shuo Tian and others, ‘Smart Healthcare: Making Medical Care More Intelligent | Elsevier Enhanced Reader’ (2019) 3 Global Health Journal <https://reader.elsevier.com/reader/sd/pii/S2414644719300508?token=2DFD351672D716CA6F7C0238A312A612A67C19A26EC8489A30588D1A0263CD4B783ECB07BEDDB375A9EE63EA4C792FDA&originRegion=eu-west-1&originCreation=20210520112219>

SL G, N F and S R, ‘EU Action for Health - Everything You Always Wanted to Know about European Union Health Policies but Were Afraid to Ask’ (2019) 3 European Observatory on Health Systems and Policies <https://www.ncbi.nlm.nih.gov/books/NBK551073/>

Smuha NA and others, ‘How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission’s Proposal for an Artificial Intelligence Act’ [2021] SSRN

Electronic Journal <https://papers.ssrn.com/abstract=3899991>

Stokke R, 'The Personal Emergency Response System as a Technology Innovation in Primary Health Care Services: An Integrative Review'

Symons J and Alvarado R, 'Can We Trust Big Data? Applying Philosophy of Science to Software' (2016) 3 Big Data and Society

Taddeo M, 'Trust in Technology: A Distinctive and a Problematic Relation' (2010) 23 Knowledge, Technology & Policy 2010 23:3 283 <https://link.springer.com/article/10.1007/s12130-010-9113-9>

Taddeo M and Floridi L, 'How AI Can Be a Force for Good' (2018) 361 Science 751 <https://www.science.org/doi/abs/10.1126/science.aat5991>

Taralunga DD and Florea BC, 'A Blockchain-Enabled Framework for Mhealth Systems' (2021) 21 Sensors
The GDPR and the Artificial Intelligence Regulation – It Takes Two to Tango? - CITIP Blog' <https://www.law.kuleuven.be/citip/blog/the-gdpr-and-the-artificial-intelligence-regulation-it-takes-two-to-tango/>

'The Pathologies of Big Data'

Thorogood A and others, 'Genetic Database Software as Medical Devices' (2018) 39 Human Mutation 1702

'Genetic Database Software as Medical Devices' (2018) 39 Human Mutation 1702

van der Sloot B and van Schendel S, 'Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study' (2016) 7 Journal of Intellectual Property, Information Technology and Electronic Commerce Law <https://heinonline.org/HOL/Page?handle=hein.journals/jipitec7&id=116&div=16&collection=journals>

Van der Sloot B and De Groot A, The Handbook of Privacy Studies: An Interdisciplinary Introduction (Amsterdam University Press 2018) <https://www.aup.nl/en/book/9789462988095/the-handbook-of-privacy-studies>

Varshney U, Nickerson R and Muntermann J, 'Taxonomy Development in Health-IT' [2013] AMCIS,2013,Proceedings <https://aisel.aisnet.org/amcis2013/HealthInformation/GeneralPresentations/15>

Vayena E and others, 'Policy Implications of Big Data in the Health Sector.' (2018) 96 Bulletin of the World Health Organization 66 <http://www.ncbi.nlm.nih.gov/pubmed/29403102>

Gasser U and others, Digital Tools against COVID-19: Taxonomy, Ethical Challenges, and Navigation Aid' (2020) 2 The Lancet Digital Health e425 <www.thelancet.com/digital-health>

Veale M and Borgesius FZ, 'Demystifying the Draft EU Artificial Intelligence Act' http://arxiv.org/abs/2107.03721

Verma AK and Prakash S, 'The Commission against the Internal Market and EU Citizens Rights: Trying to Shoot down Sputnik with the "Digital Green Certificate"?' (2020) 09 7352
Vollmer N, 'Article 4 EU General Data Protection Regulation (EU-GDPR)' <http://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm>

Waeyenberge A Van and Restrepo D, 'James Elliot Construction : A " New (Ish) Approach " to Judicial Review of Standardisation' [2017] European Law Review
Wearable Computing | The Encyclopedia of Human-Computer Interaction, 2nd Ed. <https://www.interaction-design.org/literature/book/the-encyclopedia-of-human-computer-interaction-2nd-ed/wearable-computing>

Wesolowski A and others, 'Connecting Mobility to Infectious Diseases: The Promise and Limits of Mobile Phone Data' (2016) 214 Journal of Infectious Diseases S414 <https://academic.oup.com/jid/article/214/suppl_4/S414/2527905>

Willis H. Ware, Records, Computers, and the Rights of Citizens: Report, vol 10 (Department of Health and Education of the United States of America ed, 1973)

The Wealth of Networks : How Social Production Transforms Markets and Freedom (New Haven [Conn] : Yale University Press, 2006)

Zarsky TZ, 'Incompatible: The GDPR in the Age of Big Data' (2016) 47 Seton Hall Law Review<https://heinonline.org/HOL/Page?handle=hein.journals/shlr47&id=1019&div=37&collection=journals>

Yochai Benkle'Attribute: A AND E Initial Assessment Triage Category' <https://www.datadictionary.nhs.uk/data_dictionary/attributes/a/a_and_e_initial_assessment_triage_category_de.asp?shownav=1>

Reports

Global AI Market for Healthcare Applications 2018 and 2022, Statista <https://www.statista.com/statistics/743877/worldwide-artificial-intelligence-market-healthcare-application/>

Artificial Intelligence and Machine Learning in Software as a Medical Device, FDA' <https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device>

Digital Health – OECD <https://www.oecd.org/health/digital-health.htm>

ICT Security Certification Opportunities in the Healthcare Sector, (2018) https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications%250Ahttps://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications/%250Ahttps://www.enisa.europa.eu/publications/healthcare-certificat

EU Commission, 'Manual on Borderline and Classification in the Community Regulatory

Framework for Medical Devices (Version 1.22)', vol 22 (2019)

Europe's Digital Decade: Digitally Empowered Europe by 2030 <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983>

European Commission, 'Study on Big Data in Public Health, Telemedicine and Healthcare | Digital Single Market' (2016) <https://ec.europa.eu/digital-single-market/en/news/study-big-data-public-health-telemedicine-and-healthcare>

Mobile Applications to Support Contact Tracing in the EU's Fight against COVID-19 Progress Reporting June 2020 (2020)

European Data Strategy, European Commission' <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en#documents>

European Union Agency for Fundamental Rights F, 'Coronovirus Pandemic in the EU – Fundamental Rights Implications: With a Focus on Contact-Tracing Apps' Feedback from: ETUC <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13099-Standardisation-strategy/F2663296_en>

FRA - European Union Agency For Fundamental Rights- Coronavirus Pandemic in The EU - Fundamental Rights Implications (Poland), Bulletin #1 2020, 'Coronavirus Pandemic in The EU - Fundamental Rights Implications (Poland)' (2020)

Gartner, 'Big Data' <https://www.gartner.com/en/information-technology/glossary/big-data>

'Gartner Hype Cycle For Emerging Technologies 2015' <https://www.gartner.com/smarterwithgartner/whats-new-in-gartners-hype-cycle-for-emerging-technologies-2015>

Good Machine Learning Practice for Medical Device Development: Guiding Principles, FDA <https://www.fda.gov/medical-devices/software-medical-device-samd/good-machine-learning-practice-medical-device-development-guiding-principles>

Health in the 21st Century (OECD 2019) <https://www.oecd-ilibrary.org/social-issues-migration-health/health-in-the-21st-century_e3b23f8e-en>

Hype Cycle for Emerging Technologies, 2011' <https://www.gartner.com/en/documents/1754719/hype-cycle-for-emerging-technologies-2011>

Hype Cycle for Emerging Technologies, 2013' https://www.gartner.com/en/documents/2571624/hype-cycle-for-emerging-technologies-2013

Q&A: Adoption of Regulation on Health Technology Assessment <https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_6773>

Statement on Restrictions on Data Subject Rights in Connection to the State of Emergency 1 in Member States https://net.jogtar.hu/jogszabaly?docid=a2000179.kor

Trust in Government - OECD <https://www.oecd.org/gov/trust-in-government.htm>

Valutazione d'impatto Sulla Protezione Dei Dati Personali Presentata Dal Garante Privacy <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9357972>

The Commission, 'Communications from the Commission to the European Parliament: A European Strategy for Data'<https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066>

The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)' (2021) 4 J 2021, Vol. 4, Pages 589-603 589 <https://www.mdpi.com/2571-8800/4/4/43/htm>

Data Protection Certification Mechanisms: Study on Articles 42 and 43 of the Regulation (EU) 2016/679. Final Report,(2019) https://ec.europa.eu/info/sites/info/files/data_protection_certification_mechanisms_study_final.pdf

Wearable Tech Is Being Used to Stem Outbreaks of COVID-19, World Economic Forum <https://www.weforum.org/agenda/2020/05/elderly-home-wearables-contact-tracing-apple-google>

News Articles

5G-Enabled Smart Healthcare Services Make a Huge Difference in Our Lives: No More "Getting There Too Late", Light Reading <https://www.lightreading.com/5g-enabled-smart-healthcare-services-make-a-huge-difference-in-our-lives-no-more-getting-there-too-late/a/d-id/753363>

A Harmonised European (Technical) Standard-Provision of EU Law! (Judgment in C-613/14 James Elliott Construction), European Law Blog'<https://europeanlawblog.eu/2017/01/24/a-harmonised-european-technical-standard-provision-of-eu-law-judgment-in-c-61314-james-elliott-construction/>

FDA Releases Guiding Principles for Good Machine Learning Practice, American College of Radiology <https://www.acr.org/Advocacy-and-Economics/Advocacy-News/Advocacy-News-Issues/In-the-Oct-30-2021-Issue/FDA-Releases-Guiding-Principles-for-Good-Machine-Learning-Practice>

AI: Decoded: The World's First AI Treaty — Timnit Gebru's New Gig — The European Parliament Starts Work on the AI Act – POLITICO <https://www.politico.eu/newsletter/ai-decoded/the-worlds-first-ai-treaty-timnit-gebrus-new-gig-the-european-parliament-starts-work-on-the-ai-act-2/>

Covid-19: A New Struggle over Privacy, Data Protection and Human Rights? – European Law Blog' <https://europeanlawblog.eu/2020/05/04/covid-19-a-new-struggle-over-privacy-data-protection-and-human-rights/>

Covid: EU's von Der Leyen Admits Vaccine Rollout Failures - BBC News <https://www.bbc.com/news/world-europe-56009251> accessed 13 December 2021
'Data Protection | European Commission' <https://ec.europa.eu/info/law/law-topic/data-protection_en>

Decision Zambrano v. France - Application Which Was Challenging the French "Health Pass"' <https://hudoc.echr.coe.int/eng-press#%7B%22itemid%22:[%22003-7145978-9686694%22]%7D>

Digital Solutions, European Commission <https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/digital-solutions_en>

EU Action for Health - Everything You Always Wanted to Know about European Union Health Policies but Were Afraid to Ask - NCBI Bookshelf <https://www.ncbi.nlm.nih.gov/books/NBK551073/>

L'European Commission Promuove ISDP©10003 https://www.in-veo.com

Health Data Breach: DEDALUS BIOLOGIE Fined 1.5 Million Euros, CNIL <https://www.cnil.fr/en/health-data-breach-dedalus-biologie-fined-15-million-euros> /it/news-it/461-l-european-commission-promuove-isdp-10003>

Medical Devices 2030 - KPMG (18 January 2021) <https://home.kpmg/it/it/home/insights/2018/01/medical-devices-2030.html>

Re-Open EU <https://reopen.europa.eu/en/map/LVA/6001>

Remote or Wearable Patient Monitoring Devices EUAs. FDA <https://www.fda.gov/medical-devices/coronavirus-disease-2019-covid-19-emergency-use-authorizations-medical-devices/remote-or-wearable-patient-monitoring-devices-euas>

Statement from Jeff Shuren, M.D., J.D., Director of the Center for Devices and Radiological Health, on Updated Safety Communication about Rates of Duodenoscope Contamination from Preliminary Postmarket Data | FDA' <https://www.fda.gov/news-events/press-announcements/statement-jeff-shuren-md-jd-director-center-devices-and-radiological-health-updated-safety>

Statement on the Processing of Personal Data in the Context of the COVID-19 Outbreak. European Data Protection Board, https://edpb.europa.eu/news/news/2020/statement-processing-personal-data-context-covid-19-outbreak_en

Tech Tent: Can We Learn about Coronavirus-Tracing from South Korea? BBC News <https://www.bbc.com/news/technology-52681464>

The CNPD Adopts the Certification Mechanism GDPR-CARPA, European Data Protection Board, <https://edpb.europa.eu/news/national-news/2022/cnpd-adopts-certification-mechanism-gdpr-carpa_en>

Top 10 Health Care Innovations | Deloitte | Center for Health Solutions, <https://www2.deloitte.com/it/it/pages/life-sciences-and-healthcare/articles/top-10-health-

care-innovations.html>

Big Data .Shaping Europe's Digital Future <https://ec.europa.eu/digital-single-market/en/big-data>

Building a European Health Union,
<https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2041>

Miscellaneous

GitHub - Cov-Clear/Backend: Backend Service API' <https://github.com/cov-clear/backend>

I Codici Colore Gravità (Triage)
<http://www.salute.gov.it/portale/temi/p2_6.jsp?lingua=italiano&id=1052&area=118 Pronto Soccorso&menu=vuoto>

Immuni-Documentation/README.Md at Master Immuni-App/Immuni-Documentation · GitHub'<https://github.com/immuni-app/immuni-documentation/blob/master/README.md#analytics>

ImmunityPassport: FAQ.' <https://www.immunitypassport.co/faq> accessed 16 November 2020<https://www.cnil.fr/en/iso-27701-international-standard-addressing-personal-data-protection>

InVEo, 'International Scheme For Assessing Compliance with European Regulation 2016/679: ISDP 10003- 2020 Rev00 En.Pdf' (2020)

ISO, ISO - ISO/CD 5477 - Health Informatics —Interoperability of Public Health Emergency Preparedness and Response Information Systems –Business Rules, Terminology and Data Vocabulary' <https://www.iso.org/standard/81303.html>

ISO - ISO/AWI TS 6201 - Health Informatics — Personalised Digital Health -Framework <https://www.iso.org/standard/82107.html>

ISO - ISO/CD 5477 - Health Informatics —Interoperability of Public Health Emergency Preparedness and Response Information Systems –Business Rules, Terminology and Data Vocabulary' <https://inacal.isolutions.iso.org/standard/81303.html>

ISO 27701, an International Standard Addressing Personal Data Protection | CNIL <https://www.cnil.fr/en/iso-27701-international-standard-addressing-personal-data-protection>

NHS England. About Urgent and Emergency Care <https://www.england.nhs.uk/urgent-emergency-care/about-uec/>

Protezione Civile, 'Description of the Risk' <http://www.protezionecivile.gov.it/risk-activities/health-risk/description>

The Common Good (Stanford Encyclopedia of Philosophy)'

<https://plato.stanford.edu/entries/common-good/>

WHO.Definitions: Emergencies, (2014) <https://www.who.int/hac/about/definitions/en/>

10 Annexes

Annex A. ImmuniWeb, 'Summary of Mobile Application Security Test OWASP Mobile Top 10-Kwarantanna Domowa' (2020)

---------- [Intentionally left blank] ----------