Ensure Privacy or Promote Innovation?

A Study of the Proposed AI Act

Lisa Haraldsson

Master's Thesis in European and International Trade Law

HARN63

Spring 2023

Supervisor: Jonas Ledendal

LUND UNIVERSITY

SCHOOL OF ECONOMICS AND MANAGEMENT

Table of Contents

Abbreviations

AI	Artificial Intelligence
CFR	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CNN	Convolutional Neural Networks
COVID-19	Coronavirus Disease 2019
DL	Deep Learning
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECHR	European Convention on Human Rights
ECPR	European Charter of Patients' Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	European Union
GDPR	General Data Protection Regulation
HLEG-AI	High-Level Expert Group on Artificial Intelligence
IMCO	Committee on Internal Market and Consumer Protection
LIBE	Committee on Civil Liberties, Justice and Home Affairs
MDR	Medical Devices Regulation
ML	Machine Learning

OECD	Organization for Economic Cooperation and Development
RRF	Recovery and Resilience Facility
RWD	Real-world Data
SME	Small and Medium Enterprises
TEU	Treaty of European Union
TFEU	Treaty of the Functioning of the European Union
UN	United Nations
WHO	World Health Organisation

Foreword

I would like to dedicate my foreword to my supervisor Jonas Ledendal for insightful discussions and support during the writing of this thesis. I would also like to dedicate my forward to Hanna Glad who has helped me improve my writing and reading skills. Lastly, I would like to thank and send my best wishes to my classmates who have supported me during the writing of this thesis. No one mentioned and no one forgotten!

Lisa Haraldsson
May 2023

Abstract

Artificial intelligence (AI) within healthcare creates opportunities to save more human lives regarding the prevention and prediction of diseases. This thesis has its main focus on the proposed AI Act and in what way the proposed AI Act promotes innovation and ensures privacy concerning the collection of patient data for the prevention and prediction of diseases. Furthermore, is there a balance between the promotion of innovation and ensuring privacy in the proposed AI Act with regard to the collection of patient data for the prevention and prediction of diseases?

This thesis concludes that the proposed AI Act does promote innovation through research exceptions, regulatory sandboxes, and removing barriers for Small and Medium Enterprises (SMEs). The proposed AI Act also ensures privacy through its risk-based approach. Regarding the balance between promoting innovation and ensuring privacy, there are different opinions. One argument is that the proposed AI Act does hinder the innovation of AI because the focus of the risk-based approach is too highly valued. Another argument is that the proposed AI Act does not ensure privacy because its focus is on companies and not the end user. However, it seems that the proposed AI Act values data privacy over innovation. Whether a balance between promoting innovation and ensuring data privacy is possible to achieve is difficult to say. It remains to be seen when the proposed AI Act is a finished regulation.

1. Introduction

1.1 Background

In 2022, an article was published on Frontier's website that showed the statistics of how many people die from chronic diseases. 41 million people die from chronic diseases, which is 71% of total deaths each year.[1] Patients within healthcare have therefore started to require an early detection system to treat their diseases at an early stage. Early disease detection and risk identification can result in early treatment and positive change for the patient. For example, the patient could now have time to change his or her lifestyle to prevent the disease from spreading and breaking out.[2]

Artificial Intelligence (AI) technology could be that detection system, because AI makes it possible to prevent and predict diseases, such as chronic diseases, in advance by processing previous available data.[3] To process previously available data, the AI system could include machine learning (ML) and Convolutional Neural Networks (CNN) to anticipate the disease.[4] A study from Deloitte shows that AI technology in healthcare could potentially save 313 000 lives, save €50.6 billion, and free up 1,659 million to 1,944 million working hours every year.[5] Furthermore, the European Commission is planning to invest €1 billion per year in AI technology development.[6]

Using AI as a detection system has already been done during the coronavirus disease 2019 (COVID-19).[7] COVID-19 was identified as the most life-threatening disease, so much focus was on preventing the virus from spreading.[8] One type of AI system that was used during the COVID-19 pandemic included ML which made it possible to use data to predict the location

[1] Junaid Rashid, Saba Batool, Jungeun Kim, Muhammad Wasif Nisar, Amir Hussain, Saprna Juneja & Riti Kushwaha 'An Augmented Artificial Intelligence Approach for Chronic Diseases Prediction' (2022) Frontiers in Public Health, p. 2.

[2] Op. cit., p. 1.

[3] Op. cit., p. 2.

[4] Op. cit., p. 5.

[5] Deloitte & MedTech Europe 'The socio-economic impact of AI in healthcare' (2020) Deloitte, p. 5.

[6] Commission 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Fostering a European approach to Artificial Intelligence' COM(2021) 205 final, p. 2.

[7] Hannah van Kolfschooten 'EU regulation of artificial intelligence: Challenges for patients' rights' (2022) Common Market Law Review, p. 82.

[8] Mukhtar Al-Hashimi & Allam Hamdan *Artificial Intelligence and Coronavirus COVID-19: Applications, Impact and Future Implications* in The Importance of New Technologies and Entrepreneurship Business Development: In The Context of Economic Diversity in Developing Countries (ResearchGate 2021), p. 833.

of the next outbreak of COVID-19. The information regarding the next outbreak could then be used to run border checks. Another AI system that included ML could find effective drugs for the COVID-19 virus to prevent the disease from spreading. With help from AI technology, better prevention and early prediction systems against the COVID-19 disease could be achieved.[9]

There exists an interest in cooperation between AI and healthcare because the innovation and adoption of AI technology could save billions of lives because of prevention and early prediction of diseases.[10] At the same time put the European Union (EU) at the forefront of a very innovative industry.[11] However, AI can be a considerable risk regarding patients' fundamental rights, such as data privacy.[12] There are specific risks concerning how the AI system processes patient data. Since patient data, also called health-related data, are sensitive data the data must be handled carefully.[13] It is unclear if the current EU framework for patients' rights is sufficient for this purpose.[14] There is therefore a great need for regulation regarding AI in healthcare.

The European Commission presented the draft of an AI Act on 21 April 2021.[15] The proposed AI Act creates a horizontal legal framework for AI.[16] The proposed AI Act aims to ensure that AI systems are safe, respect existing laws on fundamental rights, such as data privacy, and promote innovation regarding AI technology (art. 1 Commission's proposed AI Act). To ensure safe AI, the proposed AI Act follows a risk-based approach.[17] This means that the proposed AI Act identifies potential risks with AI.[18] To provide a secure AI system that collects patient data for the prevention and prediction of diseases, compliance with data protection legislation, such as the General Data Protection Regulation (GDPR) and

[9] Becky McCall 'COVID-19 and artificial intelligence: Protecting health-care workers and curbing the spread' (2020) Lancet Digital Health, p. 166 et seq; Commission 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Fostering a European approach to Artificial Intelligence' COM(2021) 205 final, p. 1.
[10] Deloitte & MedTech Europe [2020], p. 7.
[11] Ibid.
[12] Kolfschooten [2022], p. 82; Michael Matheny, Sonoo Thadaney Israni, Mahnoor Ahmed & Danielle Whicher (ed) *Artificial Intelligence in Health Care: The Hope, the Hype, the Promise, the Peril* (National Academy of Medicine 2019); European Union Agency for Fundamental Rights 'Data quality and artificial intelligence: mitigating bias and error to protect fundamental Rights' (2019), FRA.
[13] Rashid, Batool, Kim, Wasif Nisar, Hussain, Juneja & Kushwaha [2022], p. 2.
[14] Kolfschooten [2022], p. 82.
[15] 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' COM(2021) 206 final.
[16] European Council 'Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights' (2022) <https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/> [Accessed: 2023-04-07].
[17] Ibid.
[18] Christopher King 'Exploring the Precautionary Principle in AI Development: Historical Analogies and Lessons Learned' (2023), Lesswrong.

fundamental rights legislation such as the Charter of fundamental rights (CFR) must be met.[19] There are currently three (3) proposals for an AI Act.[20]

The difficulties regarding the aim of the Commission's proposed AI Act are to balance safe AI technology and innovation of AI technology. According to the Prime Minister for Digitalisation and Minister of regional development, the proposed AI Act both boosts innovation and respects fundamental rights.[21] This should mean that the proposed AI Act both promotes AI technology that collects patient data for the prevention and prediction of diseases. At the same time, ensure patient data protection, such as privacy regarding the collection of patient data for the prevention and prediction of diseases. The only way to know if the Prime Minister for Digitalisation and Minister of regional development tell the truth is to investigate it further.

It is therefore of interest that this thesis will examine how the proposed AI Act promotes innovation and ensures privacy with regard to the collection of patient data for the prevention and prediction of diseases. Furthermore, is there a balance between the proposed AI Act's two (2) aims, or does one (1) outweigh the other?

1.2 Purpose and Research Question

The purpose of this thesis is to describe and analyze how the proposed AI Act promotes innovation and ensures privacy with regard to the collection of patient data for the prevention and prediction of diseases.[22]

To fulfill the purpose set out above, the following research questions will be answered:

[19] Michele Ciancimino 'AI-Based Decision-Making Process in Healthcare - Towards a More Consistent Processing of Personal Data' (2022), EuCML, p. 175.

[20] 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' COM(2021) 206 final; European Council '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' (General approach) (2022); Committee on the Internal Market and Consumer Protection & Committee on Civil Liberties & Justice and Home Affairs 'Draft Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts' (2023).

[21] European Council 'Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights' (2022) <https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/> [Accessed: 2023-04-07].

[22] See further interesting thesis on similar topics, Erik Österman 'Legal Regulation for Artificial Intelligence in the European Union - Major Aspects for Minor' (2022), Lund University; Dino Ekdal 'Normative Power Europe & AI: How the EU intends to normatively govern artificial intelligence technologies through the Artificial Intelligence Act and its "trustworthy" and "human-centric" approach' (2021), Lund University; Kristina Christensen 'Exhibiting transparency without opening the 'Black Box' - Balancing act between Data Protection and Trade Secrets Rights in Solely Automated Decision-Making AI system in Healthcare' (2020), Lund University.

I. In what way does the proposed AI Act promote innovation with regard to the collection of patient data for the prevention and prediction of diseases?

II. In what way does the proposed AI Act ensure privacy with regard to the collection of patient data for the prevention and prediction of diseases?

III. Is there a balance between ensuring privacy and promoting innovation in the proposed AI Act with regard to the collection of patient data for the prevention and prediction of diseases?

1.3 Materials and Method

To fulfill the purpose of this thesis, a legal dogmatic method is used combined with an EU-legal method. There is tension between different scholars on when and how to use these methods.[23] The tension is because there is not one way of using a legal dogmatic method or an EU-legal method. There are several ways of using these methods, which therefore create tension between different interpretations of when and how to use the method.[24] This thesis follows Jan Kleineman's interpretation of a legal dogmatic method and Jane Reichel's interpretation of an EU-legal method in Maria Nääv and Mauro Zamboni's (ed) book *Juridisk metodlära.*[25]

The legal dogmatic method has been practiced for a very long time and looks generally at a concrete legal problem.[26] It is the connection between the concrete situation and the often abstract legal rule that gives the legal dogmatic method its special character.[27] Furthermore, the legal dogmatic method analyzes current law and can be used to criticize the legal situation and propose changes.[28]

The purpose of a legal dogmatic method according to Kleineman is to solve a legal problem by using legal rules.[29] Legal rules analyzed together are essential to solve a legal problem.[30]

[23] See Stig Strömholm, Max Lyles & Filippo Valguarnera *Rätt, rättskällor och rättstillämpning. En lärobok i allmän rättslära* (Norstedts Juridik 2020); Aleksander Peczenik *Juridikens teori och metod* (Norstedts Juridik 1995); Jan Hellner *Metodproblem i rättsvetenskapen. Studier i förmögenhetsrätt* (Jure 2001).

[24] See Nils Jareborg 'Rättsdogmatik som vetenskap' (2004), SvJT, p. 9 who argues that the legal dogmatic method is not a method but instead an analysis with a scientific purpose. Or Åsa Gunnarsson & Eva-Maria Svensson *Rättsdogmatik: som rättsvetenskapligt perspektiv och metod* (Studentlitteratur 2023), who sees legal dogmatic as a perspective and not a theory.

[25] Maria Nääv & Mauro Zamboni (ed) *Juridisk metodlära* (Studentlitteratur 2018), p. 21 & 109; Gunnarsson & Svensson [2023], p. 10 et seq. refers to Kleineman and Reichel which makes the source still relevant although it was published in 2018.

[26] Nääv & Zamboni [2018], p. 23 & 46.

[27] Op. cit., p. 26.

[28] Op. cit., p. 24 & 36.

[29] See Gunnarsson & Svensson [2023], p. 108 et seq.

[30] Nääv & Zamboni [2018], p. 24 & 29.

The execution will be to use generally accepted rules of law within the legal source doctrine.[31] Accepted rules of law within the legal source doctrine are legislation, jurisprudence, legislative works, and doctrine.[32] Legislation and jurisprudence from the higher court, such as the European Court of Justice (CJEU), have formal authority. Legislative work could have formal authority but generally are legislative work and doctrine used to convince by its argumentation.[33] The doctrine has especially great meaning to describe the legal situation.[34]

It can be expressed that the legal dogmatic method provides a toolbox for solving legal problems.[35] The toolbox consists of accepted rules of law within the legal source doctrine. The legal dogmatic method is suitable for this thesis because the author uses a toolbox with legal rules to answer the research questions. For example, the toolbox consists of current legislation such as the GDPR, jurisprudence from the CJEU, legislative works, such as White Paper from the European Commission, and doctrine such as academic articles regarding AI technology and patient data protection. However, the legal dogmatic method is combined with an EU-legal method to fully answer the research questions.

The EU was created by independent states choosing to cooperate in certain areas. The EU is thus an international organization and has its roots in international law.[36] The EU distinguishes primary law and secondary law.[37] Primary law consists of the treaties, such as the Treaty of the Functioning of the European Union (TFEU) and the Treaty of European Union (TEU). Secondary law contains inter alia of regulations, directives, and recommendations. If there is a tension between primary law and secondary law, primary law has precedence (art. 263 TEUF).[38] EU law has supremacy over national law, which means that in case of ambiguity, EU law must be followed over national law.[39] Furthermore, EU law concerns both the Member States and the individual because of the principle of direct effect.[40] Both individuals and Member States, therefore, need to comply with EU law.[41]

[31] See Gunnarsson & Svensson [2023], p. 108 et seq.
[32] Nääv & Zamboni [2018] p. 21 & 26.
[33] Op. cit., p. 28.
[34] Op. cit., p. 34.
[35] Op. cit., p. 24.
[36] Op. cit., p. 109.
[37] See Jörgen Hettne & Ida Otken Eriksson *EU-rättslig metod: teori och genomslag i svensk rättstillämpning* (Norstedts juridik 2011), p. 42.
[38] Op. cit., p. 41 et seq.
[39] C-6/64 *Costa v. ENEL* [EU:C:1964:66]; Damian Chalmers, Gareth Davies & Giorgio Monti *European Union Law* (Cambridge University Press 2019), p. 209.
[40] C-26/62 *Van Gend en Loos v. Administratie der Belastingen* [EU:C:1963:1]; See Justine Pila & Paul Torremans *European Intellectual Property Law* (Oxford University Press 2019), p. 37 et seq.
[41] Ibid.

Reichel sees the EU-legal method as an approach to dealing with EU legal sources.[42] EU legal sources are EU law, such as treaties and regulations, principles[43], such as the principle of conferral, case law from for example the CJEU, and soft law, such as opinions and recommendations from an EU organ.[44] Regulations and directives are legally binding.[45] The same applies to legal principles and case law from the CJEU and the Tribunal.[46] Principles have been developed through the case law of the CJEU.[47] The special character of EU law is to a large extent the result of the creative and law-making activity of the EU courts, also called the unwritten right.[48] Case law has put the purpose and place of the EU legal provisions in the forefront.[49] Case law from the CJEU, therefore, plays a crucial role in the EU-legal method.[50] One should note that the focus of this thesis is on the proposed AI Act, which is still a proposal so any case law regarding the proposed AI Act does not yet exist. Although, case law regarding patient data protection has been used for this thesis.[51] Moreover, soft laws such as recommendations are non-binding (art. 288 TFEU). Although, soft law is frequently used within the EU.[52] However, it was in the case of Luwage when the CJEU for the first time stated the legal effects of non-binding acts.[53] The CJEU stated that the non-binding act had a legal effect because it constituted rules of action.[54]

An EU-legal method is suitable for this thesis because it deals with EU-legal sources. EU law, principles, case law, and soft law from the EU. Furthermore, combining a legal dogmatic method and an EU-legal method makes it possible to fulfill the purpose of this thesis and give the answers to the research questions. Does the proposed AI Act promote innovation and ensure privacy with regard to the collection of patient data for the prevention and prediction of diseases, and is there a balance between these two (2)? This is because a legal situation is analyzed with help from legal rules and EU legal sources.

The material for this thesis mainly consists of the proposed AI Act and doctrine regarding the proposed AI Act. The material for this thesis was collected up to 25 May 2023. The material

[42] Nääv & Zamboni [2018], p. 109.
[43] Note, there are different degrees of principles such as general and specific, see Hettne & Eriksson [2011], p. 63.
[44] See Nääv & Zamboni [2018], p. 109 et seq.
[45] Pila & Torremans [2019], p. 60 et seq.
[46] Hettne & Eriksson [2011], p. 40.
[47] Chalmers, Davies & Monti [2019], p. 260.
[48] Hettne & Eriksson [2011], p. 40.
[49] Op. cit., p. 49.
[50] See Nääv & Zamboni [2018], p. 131; Hettne & Eriksson [2011], p. 41 & 49.
[51] See Nääv & Zamboni [2018], p. 128.
[52] Hettne & Eriksson [2011], p. 46 et seq.
[53] C-148/73 *Raymond and Marie Louwage.* [ECLI:EU:C:1974:7].
[54] Hettne & Eriksson [2011], p. 48.

after this date has therefore not been taken into account. The reason is that the thesis was submitted on 26 May 2023.

1.4 Structure

Chapter two (2) covers AI. Different definitions of AI are put forward. AI technology for the prevention and prediction of diseases is described as creating a greater understanding of the aspect of innovation and patient data protection. Followed by challenges with AI technology to ensure privacy and promote innovation with regard to the collection of patient data for the prevention and prediction of diseases. Furthermore, the background of the proposed AI Act and its purpose are described. The proposed AI Act's recitals and articles are described in more detail concerning ensuring privacy and promoting innovation with regard to the collection of patient data for the prevention and prediction of diseases. Finally, a summary of the chapter is presented.

Chapter three (3) introduces patient data protection. A description of patient data protection as a fundamental right and within data protection regulation. Chapter three gives the background required regarding patient data protection and data privacy to further understand chapter four (4) and the third (3) research question. Is there a balance between the promotion of innovation and ensuring privacy in the proposed AI Act with regard to the collection of patient data for the prevention and prediction of diseases? Finally, a summary of the chapter is presented.

Chapter four (4) covers the balance between promoting innovation and ensuring privacy in the proposed AI Act, with regard to the collection of patient data for the prevention and prediction of diseases. Criticism and opinions are described concerning if the proposed AI Act both ensures privacy and promotes innovation with regard to the collection of patient data for the prevention and prediction of diseases. The chapter ends with a summary.

Chapter five (5) contains a concise summary and conclusion. Since chapters two (2), three (3), and four (4) contain summaries, chapter five (5) is kept short. The author's opinion is stressed in this chapter.

2. Artificial Intelligence

2.1 Introduction

This chapter provides the reader with a background to AI and the proposed AI Act. There is currently no universal definition of AI. The most prominent definitions are mentioned in this chapter as well as which definition will be followed for this thesis. Furthermore, AI technology that collects patient data for the prevention and prediction of diseases is described. Followed by the challenges of AI technology regarding ensuring privacy and promoting innovation with regard to the collection of patient data for the prevention and prediction of diseases.

The chapter continues with a description of the proposed AI Act. How the proposed AI Act came about and its current status. Furthermore, the purpose and aim of the proposed AI Act. Followed by a description of the recitals and articles dealing with ensuring privacy and promoting innovation with regard to the collection of patient data for the prevention and prediction of diseases. The chapter ends with a summary.

2.2 What is Artificial Intelligence?

2.2.1 Introduction

What is AI? This could be seen as an easy question but AI has different definitions because of the complexity of the technique and its continuous development. However, it is important to define AI to understand what is covered by the term. Not least for regulating the technology. This thesis addresses three (3) different definitions of AI.[55]

Firstly, according to the European Commission's High-Level Expert Group on Artificial Intelligence (HLEG-AI), the definition of AI could be described as:

> *"[...] software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and*

[55] There are of course several definitions of an AI system.

> *deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.*
>
> *As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems).”*[56]

The HLEG-AI definition of AI is quite broad and includes various aspects of AI. This allows the definition to cover a broad area concerning AI and its innovation. However, the definition is quite technical and not technology neutral, which can be a disadvantage if the definition is to be innovative-friendly.

Secondly, the Organization for Economic Cooperation and Development (OECD) defines AI as a ”machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.”[57] The OECD definition is short but still broad and vague, compared to the HLEG-AI definition of AI which is more extensive and technical.

Thirdly, a definition of AI is also found in the Committee on the Internal Market and Consumer Protection (IMCO) and Committee on Civil Liberties, Justice and Home Affairs (LIBE) proposed AI Act[58], which state:

> *”[...] a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments.”*[59]

The definition of AI in the IMCO and LIBE proposed AI Act is similar to the OECD definition of AI. However, the IMCO and LIBE proposed AI definition is broad but clear.

[56] High-Level Expert Group on Artificial Intelligence ‘A definition of AI: Main capabilities and disciplines - Definition developed for the purpose of the deliverables of the High-Level Expert Group on AI’ (2018), Commission, p, 6.

[57] OECD ‘Recommendation of the Council on Artificial Intelligence’ (2019), I.

[58] Committee on the Internal Market and Consumer Protection (IMCO) & Committee on Civil Liberties & Justice and Home Affairs (LIBE) ‘Draft Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts’ (2023).

[59] Art. 3 of the IMCO & LIBE proposed AI Act.

IMCO and LIBE's vague definition is a consequence of the aim to make the proposed AI Act flexible to new innovations regarding AI technologies (recital 6 IMCO and LIBE proposed AI Act). This thesis will follow the IMCO and LIBE proposed definition of AI. This is because the IMCO and LIBE definition of AI is innovative-friendly and therefore well equipped regarding the development of AI technology.

2.2.2 Artificial Intelligence Technology

AI within healthcare has over the past years increased significantly regarding research and development of AI technology.[60] The COVID-19 pandemic accelerated the development and deployment of AI applications, as AI-related technologies were the central core of the response to this worldwide health crisis.[61] One reason for the increase is that AI can process lots of data (Big Data) for the prevention and prediction of diseases.[62] Nevertheless, AI systems have a lot of attention, but what exactly is AI technology?

AI covers several approaches and techniques.[63] For example, ML is a statistical technique for fitting models to data and learning by training models with data.[64] The human contribution to the ML process is generally limited to writing the initial algorithm and supervising the AI during its learning process.[65] ML is one of the most common techniques regarding AI. A complex form of ML is neural networks, this technique views problems in terms of inputs, outputs, and weights of variables or features that associate input with output.[66] The AI system will produce different outputs based on the input data.[67] A further complex form of ML is deep learning (DL) which includes levels of features/variables that predict outcomes. There can be hidden features when using DL.[68] Moreover, decentralized AI is relatively new to ML. Decentralized AI opens up the opportunity for several parties to jointly train an ML model without collecting data, such as patient data, centrally for training. A common form of decentralized ML is federated ML. Thus, federated ML, a type of decentralized AI, can be used by multiple actors without patient data being exchanged between them. An example where this technique is useful is when actors individually have insufficient training data to

[60] Kolfschooten [2022], p. 90.
[61] European Parliament 'Artificial intelligence in healthcare - Applications, risks, and ethical and societal impacts' (2022), EPRS, p. 1.
[62] Thomas Davenport & Ravi Kalakota 'The potential for Artificial intelligence in healthcare' (2019), Future Healthcare Journal, p. 94.
[63] Ibid.
[64] See Ethem Alpaydin *Introduction to Machine Learning* (MIT Press 2020), p. 3.
[65] Gabriele Spina Ali & Ronald Yu 'Artificial Intelligence between Transparency and Secrecy: From the EC Whitepaper to the AIA and Beyond' (2021), EJLT, p. 3.
[66] For further reading, Alpaydin [2020], p. 4-13.
[67] Ali Spina & Yu [2021], p. 3.
[68] Davenport & Kalakota [2019], p. 94.

achieve an acceptable performance.[69] It is argued that decentralized AI should be promoted to support Big Data in healthcare because there is no need for data transfers, which could be unsafe.[70]

There are techniques other than those mentioned above when it comes to AI, for example in robotics. Robotics will however not be further described because this thesis focuses on AI that collects patient data for the prevention and prediction of diseases. Robotics is instead frequently used for administration or the treatment itself.[71]

Regarding the collection of patient data for the prevention and prediction of diseases, wearables, imaging, physiological monitoring, real-world data (RWD), and personalized apps are relevant AI technologies.[72] Wearables could be a smartwatch, accelerometer bracelets, or biosensors. This wearable could be used to prevent heart failure.[73] Regarding imaging, AI as ML could predict potential diseases for patients by analyzing images together with clinical data. For example, images to detect breast cancer.[74] Physiological monitoring makes it possible to predict health advances. The AI system could detect rapid physiologic changes in critically ill patients ahead of time. Thereafter, come up with a treatment plan to prevent the disease. A concrete example of AI and physiological monitoring is eye-tracking technologies. Today, the doctor needs to analyze the patient’s eye movement to assess brain health. Eye-tracking technologies, which is a form of AI monitoring application, linked to ML, have helped predict neurological impairment faster and with more precision by analyzing the retina of the patient. This early detection results in that the patient now doesn’t need eye drops for dilation.[75] RWD and AI-generated insight could improve the prevention of diseases by collecting patient data. RWD contains smart technologies for everyday activities. RWD together with predictive AI models (including ML and DL) could link multiple data sources and as a result, identify patients more likely to respond to a specific treatment.[76] Personalized apps with AI technology could prevent treatment for a patient by providing intensive ad-hoc

[69] Integritetsskyddsmyndigheten ‘Federerad maskininlärning mellan två vårdgivare - Slutrapport om Integritetsskyddsmyndighetens pilotprojekt med regulatorisk testverksamhet om dataskydd’ (2023), IMY, p. 8.

[70] European Parliament ‘Artificial intelligence in healthcare - Applications, risks, and ethical and societal impacts’ (2022), EPRS, p. 24 et seq.

[71] AL-Hashimi & Hamdan [2021], p. 836.

[72] Deloitte & MedTech [2020], p. 14.

[73] Op. cit., p. 17.

[74] Op. cit., p. 18.

[75] Op. cit., p. 22.

[76] Op. cit., p. 24 et seq.

behavior counseling to help the patient change his or her health-related behavior. An example is personalized eating plans.[77]

AI technology such as ML, DL, or decentralized contributes great opportunities and contributions within health to prevent and predict diseases. However, great opportunities also come with great risks and challenges.

2.2.3 Challenges with Artificial Intelligence Technology

AI technology is subject to different legal frameworks such as Medical Devices Regulation (MDR)[78], GDPR, and the Product Liability Directive[79]. These different legal frameworks are important to establish safe AI technology regarding the collection of patient data. Especially AI that collects Big Data to make predictions and prevent diseases.[80] It is crucial that the processed data is of high quality to not create a biased and unsafe AI. Within healthcare, it is even more important to ensure the high quality of the collected data. This is because patient data is a form of sensitive data. This means that patient data is under strict privacy data protection regulations, such as the GDPR.

However, most of the data is currently held in silos which makes it hard for stakeholders to transfer or compare the data. Regardless, for a medical AI solution, existing data must be carefully evaluated to ensure it meets the requirements of high quality, accuracy, representative, and interpretable.[81] The term accuracy is usually interpreted as the correctness of personal data for one individual, although the term accuracy could be interpreted more widely.[82]

Patient data is also an attractive target for cybercriminals. There has been an increased lack of public trust regarding data privacy because of rising cyber attacks and hacking of health records databases.[83] The cyberattacks could lead to personal information being made widely available, infringing the right to privacy and putting the patient at risk.[84] For example, a

[77] Deloitte & MedTech [2020], p. 28.

[78] 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/EEC.

[79] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

[80] An example is Google Translate which uses a statistical machine engine that identifies linguistic patterns in millions of United Nations and EU Parliament documents. See Ali Spina & Yu [2021], p. 4.

[81] Deloitte & MedTech [2020], p. 31.

[82] European Union Agency for Fundamental Rights [2019], p. 9.

[83] Sally Dalton-Brown 'The ethics of medical AI and the physician-patient relationship' (2020), Cambridge Quarterly of Healthcare Ethics, p. 116; Tjasa Zapusek 'Artificial intelligence in medicine and confidentiality of data' (2017), Asia Pacific Journal of Health Law and Ethics, p. 105.

[84] Steve Alder 'AI Company Exposed 2.5 Million Patient Records Over the Internet' (2020), HIPPA Journal.

patient died in 2020 after having to be redirected to another hospital because the first hospital suffered a cyberattack. This cyberattack interfered with the hospital data and rendered the hospital computer system inoperable.[85] Although it was later argued that the cyber attack could not be directly linked to the patient's death because the patient was already before the cyberattack in a life-threatening condition.[86] It is however important to meet the cybersecurity standards, which some hospitals may not do.[87]

Data privacy is a concern regarding medical AI.[88] Such as challenges regarding trust, governance, and patient empowerment.[89] The AI system could, for example, regard Big Data share and use personal data without informed consent from the patient.[90] Furthermore, the risk of data re-purposing without the patient's knowledge.[91] An example of data being transferred was in 2016 when a patient record of 1.6 million was transferred from the Royal Free NHS Foundation Trust to Google's DeepMind without the patient's informed consent.[92] This transaction without the patient's consent broke against data protection laws.[93] Informed consent is linked to various ethical issues, such as privacy protection, and property rights concerning data.[94] Informed consent is a crucial and integral part of the patient's experience in healthcare.[95] However, informed consent could form a limit regarding the level of autonomy and possibility to share patient decision-making.[96]

HLEG-AI has provided a checklist regarding data privacy. The checklist states that compliance with Data Protection Impact Assessment (DPIA) is needed. Designation of a Data Protection Officer (DPO) and inclusion at an early stage in the development, procurement, or use of the AI system. Moreover, measures to achieve privacy by design and default, such as

[85] Maximilian Kiener 'You may be hacked' and other things doctors should tell you' (2020) <https://theconversation.com/you-may-be-hacked-and-other-things-doctors-should-tell-you-148946> [Accessed: 2023-05-15].

[86] European Parliament 'Artificial intelligence in healthcare - Applications, risks, and ethical and societal impacts' (2022), EPRS, p. 25.

[87] Deloitte & MedTech [2020], p. 31.

[88] Dalton-Brown [2020], p. 116; Zapusek [2017], p. 105.

[89] Further reading, Deloitte & MedTech [2020], p. 32.

[90] Alex McKeown, Miranda Mourby, Paul Harrison, Sophie Walker, Mark Sheehan & Ilina Singh 'Ethical issues in consent for the reuse of data in health data platforms'(2021), Science and Engineering Ethics.

[91] European Parliament 'Artificial intelligence in healthcare - Applications, risks, and ethical and societal impacts' (2022), EPRS, p. 24; Brian Pickering 'Trust, but Verify: Informed Consent, AI Technologies, and Public Health Emergencies, Future Internet' (2021), MDPI, p. 132.

[92] BBC 'Google DeepMind NHS app test broke UK privacy law' (2017) <https://www.bbc.com/news/technology-40483202> [Accessed: 2023-05-15].

[93] Sara Gerke, Timo Minssen & Glenn Cohen 'Ethical and legal challenges of artificial intelligence-driven healthcare' (2020), Academic Press, p. 295-336.

[94] Thomas Ploug & Sören Holm 'Meta Consent –A Flexible Solution to the Problem of Secondary Use of Health Data' (2016), Bioethics.

[95] Pickering [2021].

[96] Debra Malina (ed) 'Hidden in Plain Sight — Reconsidering the Use of Race Correction in Clinical Algorithms' (2020), The New England Journal of Medicine, p. 874 et seq.

anonymization have to be implemented. Also, implementation of the right to withdraw consent, the right to object, and the right to be forgotten into the development of the AI system.[97] This checklist could help patients to better understand the decision-making process and the different ways their data can be reused and the opportunity to opt out of sharing their data.

There are also challenges regarding decentralized AI and federated ML. There is a risk of the system remembering the training data, and the patient data.[98] There are two (2) potential solutions to prevent the system from remembering patient data. Membership Inference Attack or Model Inversion Attack.[99] Membership Inference Attack aims to find out whether a certain data point has been included in the training data or not.[100] Model Inversion Attack aims to recreate the variable values in data points from the training data.[101] However, these two (2) solutions do not eliminate the risk for the AI system to remember the data.[102]

Challenging and unsafe AI technology can be the so-called black box effect. This is when an AI system comes up with a prediction or prevention without showing how it came up with the prediction or the prevention.[103] Thus, the input and the output can be seen but without an understanding of the process itself.[104] An illustrative non-medical example is an image of a cat. It is easy to look at a picture of a cat and identify it as a cat. It is easy because we have seen many pictures of cats before and therefore know what cats look like. However, it is hard to state what a picture of a cat looks like to a person who has never seen a cat before. Moreover, it is very hard to tell a computer, hyperliteral and without any relevant experience, how to perform that task. However, computers can learn how to do this.[105]

The black box effect is particularly problematic regarding DL. For example, DL algorithms that are used for image analyzis are virtually impossible to interpret or explain.[106] The lack of explanation is problematic because the black box effect could cause problems concerning the

[97] European Parliament ‘Artificial intelligence in healthcare - Applications, risks, and ethical and societal impacts’ (2022), EPRS, p. 33.
[98] Integritetsskyddsmyndigheten [2023], p. 17 et seq; See also European Union Agency for Cybersecurity ‘Artificial Intelligence Cybersecurity Challenges. Threat Landscape for Artificial Intelligence’ (2020).
[99] Integritetsskyddsmyndigheten [2023], p. 17 et seq.
[100] Integritetsskyddsmyndigheten [2023], p. 18.
[101] Integritetsskyddsmyndigheten [2023], p. 19.
[102] European Parliament ‘Artificial intelligence in healthcare - Applications, risks, and ethical and societal impacts’ (2022), EPRS, p. 24 et seq.
[103] Kolfschooten [2022], p. 95; Yavar Bathaee ‘The artificial intelligence black box and the failure of intent and causation’ (2018), Harvard Journal of Law & Technology, p. 891 et seq.
[104] Dalton-Brown [2020], p. 117.
[105] See W. Nicholson Price II ‘Regulating black-box medicine’ (2017), Michigan Law Review, p. 430.
[106] Davenport & Kalakota [2019], p. 97.

patients' right to information.[107] For instance, if DL algorithms have analyzed an image and detected the disease cancer, the patient will most likely want to know how the system came to that conclusion.[108] This could further challenge liability. Who is to blame if the AI system generates wrong predictions and preventions.[109] It is important to establish which, by whom, and for what purpose the information regarding the patient can be used.[110]

Two (2) potential explanations for the black box effect are (1) the AI system relies on rules that are too complex for humans or (2) it is impossible to determine exactly what factors have been used for the prediction or prevention.[111] Two (2) possible solutions regarding the black box effect are to either regulate the degree of transparency that AI must exhibit or to impose strict liability for harm inflicted by AI. Both solutions are, according to Bathaee, problematic, incomplete, and likely to be ineffective levers for the regulation of AI.[112] This is because innovation will most likely be affected negatively.[113]

Another concern regarding the black box effect is discriminatory practices, which cannot be detected.[114] For example, ML systems in healthcare could see a likelihood of a disease regarding gender or race when it's not an actual causal factor.[115] Patient protection could therefore be a subject of discrimination.[116] The potential risk regarding discrimination and AI technology within health has been explicitly addressed in the EU White Paper on AI[117] and HLEG-AI Ethics Guidelines on Trustworthy AI.[118] There are previous cases where AI systems have discriminated against persons based on sex and ethical background.[119] One example where transparency regarding the AI prediction would have helped is within the patient

[107] Commission 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Fostering a European approach to Artificial Intelligence' COM(2021) 205 final, p. 2.
[108] Davenport & Kalakota [2019], p. 97.
[109] Dalton-Brown [2020], p. 116; Zapusek [2017], p. 105.
[110] See European Commission 'Ethics Guidelines for Trustworthy AI' (2019) <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> [Accessed: 2023-04-29]; Deloitte & MedTech [2020], p. 31.
[111] Kolfschooten [2022], p. 95; Nicholson Price II [2017], p. 430.
[112] Bathaee [2018], p. 893.
[113] Op. cit., p. 893 et seq.
[114] Heleen Janssen 'An approach for a fundamental rights impact assessment to automated decision-making' (2020), International Data Privacy Law, p. 92.
[115] Davenport & Kalakota, [2019], p. 97.
[116] Jonathan Cohen & Tamar Ezer 'Human rights in patient care: A theoretical and practical framework' (2013), Health and Human Rights Journal.
[117] European Commission 'White Paper On Artificial Intelligence – A European approach to excellence and trust' COM(2020) 65 final, p. 11.
[118] High-Level Expert Group on Artificial Intelligence 'Ethics Guidelines for Trustworthy AI' (2019), Commission, p. 18; Charline Daelman 'AI through a human rights lens. The role of human rights in fulfilling AI's potential' (2021), Artificial Intelligence and the Law, p. 137.
[119] Ali Spina & Yu [2021], p. 4; Daniel Gutierrez 'AI Black Box Horror Stories - When Transparency was needed' (2019) <https://opendatascience.com/ai-black-box-horror-stories-when-transparency-was-needed/> [Accessed: 2023-05-08].

diagnosis. It was in 2015 when a research group worked on DL software, also called Deep Patient software. The research group worked to apply this DL software to a hospital's large database of patient records featuring hundreds of variables on patients drawn from their test results, doctor visits, etc. The Deep Patient software was trained by 700.000 patient data to predict diseases. The Deep Patient software was able to find patterns that were hidden in the hospital data. However, Deep Patient turned out to be a black box because its predictions could not be explained.[120] However, transparency could also be seen as a hinder to AI innovation.

Challenges regarding innovation within AI technology, such as AI that collects patient data for the prevention and prediction of diseases, are foremost Intellectual Property protection. There is a risk regarding companies that develop AI technology and open up to public scrutiny that competitors' free-ride on that company's innovator-based technology. This could be seen as a hinder to innovation regarding AI technology because the companies can then not benefit from their investments.[121] These challenges are both organizational and financial because of digitalization adoption, the cost of the technology, and skills and training regarding AI applications.[122]

Lack of data privacy, confidentiality, and protection for patients and citizens could lead to serious consequences. Consequences like exposure and use of patient data, sensitive data, which goes against the rights of the patient.[123] To hinder the patient's lack of trust in the AI technology, risk assessment, classification, and management must be an integral part of the AI development, evaluation, and deployment processes.[124] Specifically, more clarity, guidance, and rules concerning AI within healthcare are required.[125]

2.3 What is the Proposed Artificial Intelligence Act?

2.3.1 Introduction

The use of AI creates a number of high risks. There is already an established legal framework to protect fundamental rights and ensure safety and data protection rights. However, existing

[120] Gutierrez [2019].
[121] Ali Spina & Yu [2021], p. 6 et seq.
[122] Further reading, Deloitte & MedTech [2020], p. 32.
[123] European Parliament 'Artificial intelligence in healthcare - Applications, risks, and ethical and societal impacts' (2022), EPRS, p. 23.
[124] Op. cit., p. 15.
[125] See European Commission 'Ethics Guidelines for Trustworthy AI' (2019) <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> [Accessed: 2023-04-29]; Deloitte & MedTech [2020], p. 31.

legislation is not sufficient and can make the application and enforcement of the proposed AI Act more challenging. To avoid this tension, the proposed AI Act introduces harmonized rules regarding the design, development, and use of certain high-risk AI systems.[126]

There are currently three different proposals for an AI Act. The Commissions[127], the Councils[128], and the Parliament's IMCO and LIBE[129]. There are both overlaps and amendments in their proposals regarding promoting innovation and ensuring privacy. The Commission's proposal will be most referred to because the numbers and content in the articles and recitals are more or less the same in all three proposals. However, amendments in the Council and the IMCO and LIBE proposals will be addressed when accurate.

2.3.2 Background to the Proposed Artificial Intelligence Act

An AI framework was prepared in October 2017.[130] The European Commission published the European approach to AI in 2018.[131] At the same time, HLEG-AI was created to support the European Commission with advice for a new AI policy. The European Commission published the White Paper on Artificial Intelligence 2020. The White Paper set out policy options for a future EU regulatory framework to safeguard an ecosystem of trust in Europe.[132] The White Paper addressed that the current EU legal framework was insufficient regarding AI.[133]

It was in 2021 when the European Commission published the legislative proposal on Artificial Intelligence, the so-called AI Act.[134] The European Council adopted its general approach to the AI Act on 6 December 2022.[135] The Parliament's IMCO and LIBE jointly

[126] Commission 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Fostering a European approach to Artificial Intelligence' COM(2021) 205 final, p. 4.

[127] 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' COM(2021) 206 final.

[128] Council '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' [General approach] (2022).

[129] IMCO & LIBE 'Draft Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts' (2023), European Parliament.

[130] See timeline, European Commission 'A European approach to artificial intelligence' <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> [Access: 2023-04-06].

[131] Ibid.

[132] Commission 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Fostering a European approach to Artificial Intelligence' COM(2021) 205 final, p. 3.

[133] Kolfschooten [2022], p. 104.

[134] Ibid.

[135] European Council 'Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights' (2022) <https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/> [Accessed: 2023-04-07].

adopted the text by a large majority on 11 May 2023.[136] The next step is plenary adoption, which has a tentative date of June 12, 2023.[137] It is not certain that the IMCO and LIBE's text will be adopted in Parliament. However, this text is valid until further notice. After plenary adoption, the proposal will enter the last stage of the legislative process, the negotiations with the EU Council and Commission, so-called trialogues.[138] The proposed AI Act may be a finished regulation by the end of 2023 and become part of the EU's regulatory system.[139]

The purpose of the proposed AI Act is to promote the uptake of human-centric and trustworthy AI and to ensure a high level of protection of health, safety, fundamental rights, democracy, and rule of law, and the environment from harmful effects of AI systems in the Union while supporting innovation (art. 1 Commission's proposed AI Act). To do that, the proposed AI Act lays down harmonized rules concerning prohibitions of certain AI practices, specific requirements for high-risk AI systems, and obligations for operators of such systems. Furthermore, harmonized transparency rules for certain AI systems and measures to support innovation. For example with a particular focus on SMEs.[140] The risk criteria in the proposed AI Act are meant as a guide for the Commission itself and not the targets of regulation.[141] The rules in the proposed AI Act would primarily apply to providers of AI systems and users of AI systems in the EU (art. 2 Commission's proposed AI Act).[142]

The proposed AI Act takes a top-down approach, compared to the GDPR which takes a bottom-up approach. A bottom-up approach means that the evaluation of risk and the choice of mitigating measures are not defined by the law. Instead, it is up primarily to the targets of the GDPR which are data controllers and processors. This approach aims to reduce the imposition of duties coming from above (principle of accountability)[143]. The top-down

[136] European Parliament 'AI Act: a step closer to the first rules on Artificial Intelligence' (2023) <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence> [Accessed: 2023-05-11].

[137] Parliament '2021/0106(COD) Artificial Intelligence Act' <https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0106(COD)&l=en> [Accessed: 2023-05-15].

[138] Luca Bertuzzi 'AI Act moves ahead in EU Parliament with key committee vote' (2023) <https://www.euractiv.com/section/artificial-intelligence/news/ai-act-moves-ahead-in-eu-parliament-with-key-committee-vote/> [Accessed: 2023-05-11].

[139] See Lucas Bertuzzi 'AI Act: European Parliament headed for key committee vote at end of April' (2023) <https://www.euractiv.com/section/artificial-intelligence/news/ai-act-european-parliament-headed-for-key-committee-vote-at-end-of-april/> [Accessed: 2023-04-25]; Kolfschooten [2022], p. 100.

[140] See also European Data Protection Board '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)' (2021).

[141] Giovanni de Gregorio & Pietro Dunn 'The European Risk-based Approaches: Connecting Constitutional Dots in the Digital Age' (2022), Common Market Law Review, p. 492.

[142] Parliament 'Artificial Intelligence act' [Briefing] (2022), p. 4.

[143] See art. 5(2) of the GDPR.

approach means that the proposed AI Act does not leave the task of evaluating the risk to the targets of the regulation, instead the proposed AI Act itself identifies the various categories of risk. The different approaches may cause regulatory fragmentation which could affect the goals of the internal market and the EU's constitutional principles. However, GDPR and the proposed AI Act share the same goal of balancing fundamental rights and innovation.[144]

2.3.3 Ensure Privacy Regarding Collection of Patient Data for the Prevention and Prediction of Diseases

Since the Digital Single Market Strategy[145] the EU increasingly relied on a risk-based approach.[146] A risk-based approach follows the precautionary principle.[147] The precautionary principle's primary goal is to minimize harm and avoid regrettable outcomes.[148] Implementing the precautionary principle in AI development would include, identifying and assessing potential risks, implementing preventive measures, monitoring and adapting, and fostering cooperation and transparency.[149] For example, the precautionary principle helps to ensure privacy regarding the collection of patient data for the prevention and prediction of diseases by establishing regulatory sandboxes.

The proposed AI Act does however not define the high-risk concept. Instead, the proposed AI Act identifies the AI system as a risk in its annexes.[150] The proposed AI Act proposes four different levels of risk. (1) Unacceptable risk, (2) high risk, (3) limited risk, and (4) minimal risk. Unacceptable AI has a high bar because the system has to cause physical or psychological damage or have the capability of doing so (art. 5(a) Commission's proposed AI Act). Art. 6 of the Commission's proposed AI Act regulates high-risk AI systems that create an adverse impact on people's safety or their fundamental rights. The Commission's proposal of an AI Act distinguishes two (2) categories of high-risk AI systems. Firstly, high-risk AI systems that are used as a safety component of a product. Secondly, high-risk AI systems as a product falling under Union health and safety harmonization legislation. AI systems that are classified as low or minimal risk can be developed and used in the EU without conforming to additional legal obligations. The proposed AI Act encourages providers of AI systems that are

[144] Gregorio & Dunn [2022], p. 476 et seq.

[145] European Commission 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Single Market Strategy for Europe' COM(2015) 192 final.

[146] See de Gregorio & Dunn [2022], p. 476.

[147] T-817/14 *Zoofachhandel Züpke and others v. Commission,* [EU:T:2016:157].

[148] King [2023].

[149] Ibid.

[150] Annex I lays out a list of techniques and approaches that are used today to develop AI and refers to machine learning, logic and knowledge-based systems, and statistical approaches.

classified as a low or minimal risk to voluntarily apply the mandatory requirements for high-risk AI systems (codes of conduct).[151]

Like the MDR, the higher the risk, the stricter the rule.[152] The proposed AI Act does not specifically address the risk level of AI in healthcare. Instead, the Commission's proposed AI Act states that all medical devices under the MDR will be classified as high-risk (recital 30-31 Commission's proposed AI Act).[153] This suggestion is based on privacy and safety aspects.[154] However, different types of health AI present different degrees of risk.[155] This could mean that health AI that does not fall under the MDR is considered a limited risk which results in minimal regulation under the proposed AI Act.[156]

Because of the high-risk approach, several conditions in art. 16 of the Commission's proposed AI Act must be met before the AI system can be put on the EU internal market.[157] The requirements in art. 16 concerns for instance compliance with the requirements set out in Chapter 2, quality management systems that comply with art. 17 of the Commission's proposed AI Act and relevant conformity assessment procedure by art. 43 of the Commission's proposed AI Act (art. 16 Commission's proposed AI Act). Furthermore, it is appropriate that a high-risk AI system undergoes a new conformity assessment whenever continuous learning may create a new unacceptable risk and significantly affect the compliance of the high-risk AI system (recital 66 Commission's proposed AI Act).

AI is a rapidly developed technology and requires regulatory oversight and a safe space for testing with human oversight (art. 14 Commission's proposed AI Act).[158] Therefore, the Commission's proposed AI Act promotes the implementation of regulatory sandboxes (art. 53-55 Commission's proposed AI Act).

Regulatory sandboxes come with a number of benefits. For instance, regulators could develop adequate rule-making, supervision, and enforcement policies due to a better understanding of the innovative products. Furthermore, avoiding potential legal risks because innovators now can develop their products and services in a regulation-compliant way (5.2.5. and recital 71

[151] European Parliament 'Artificial Intelligence act [Briefing] (2022), p. 7.
[152] See Kolfschooten [2022], p. 104 et seq.
[153] Ibid.
[154] European Parliament 'Artificial intelligence in healthcare - Applications, risks, and ethical and societal impacts' (2022), EPRS, p. 32.
[155] Kolfschooten [2022], p. 89; Janssen [2020], p. 80.
[156] Kolfschooten [2022], p. 107 et seq.
[157] See also art. 8 of the Commission's proposed AI Act.
[158] 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)' (2021), p. 6.

Commission's proposed AI Act). The ability to test new technology in a regulation-compliant way opens up the possibility to test the new technology without having to comply with all regulatory requirements, which are normally applicable. This is particularly useful for addressing innovations that do not fit an existing framework. Moreover, testing in a controlled environment could mitigate the risk of bringing new technology to the market. It could also potentially reduce the time-to-market cycle for new products.[159] Regulatory sandboxes could for example allow participants to use patient data to foster AI innovation without prejudice to the GDPR requirements (art. 55 and 69.4 Commission's proposed AI Act).[160] Regulatory sandboxes could therefore be seen to both ensure privacy and promote innovation.[161] However, participation in a regulatory sandbox does not exempt participants from liability.[162]

Furthermore, risks with regulatory sandboxes are if they are misused. This could lead to lower safeguards and requirements to attract innovators. There is also a risk regarding regulators that prioritize adequate safeguards over innovation. This could result in stifling innovation because overly restrictive regulations or fear of potential risks are prioritized. Moreover, there is a risk of fragmentation of the EU single market because of different testing parameters in different Member States.[163] To avoid fragmentation, all parties involved should aim for transparency and openness and respect the confidentiality of information and data obtained (recital 83 Commission's proposed AI Act).

Access to high data quality plays a vital role in ensuring the performance of many AI systems and ensuring that the high-risk AI system performs safely and does not discriminate. High-quality training, validation, and testing data sets require the implementation of appropriate data governance. Training, validation, and testing data should be sufficiently relevant, representative, appropriately vetted for errors, and as complete as possible regarding the purpose of the AI system (recital 44 Commission's proposed AI Act).

The right to privacy and protection of personal data must be guaranteed throughout the entire lifecycle of the AI system. In this regard, the principles of data minimization are essential when the processing of data involves significant risks to the fundamental rights of individuals. Providers and users of AI systems should implement organizational measures in order to protect the fundamental rights of individuals (recital 45(a) Commission's proposed AI Act).

[159] European Parliament 'Artificial intelligence act and regulatory sandboxes' [briefing] (2022), p. 2.
[160] European Parliament 'Artificial Intelligence act' [Briefing] (2022), p. 7.
[161] See also art. 72 of the Commission's proposed AI Act.
[162] European Parliament 'Artificial intelligence act and regulatory sandboxes' [briefing] (2022), p. 2.
[163] Ibid.

Data subjects should always be informed that they are subject to the use of a high-risk AI system when deployers use a high-risk AI system (recital 84(b) Commission's proposed AI Act).

2.3.4 Promote Innovation Regarding Collection of Patient Data for the Prevention and Prediction of Diseases

The proposed AI Act contains aspects of innovation and how innovation could be promoted regarding AI technology. One way of promoting innovation is research exceptions (recital 40 Commission's proposed AI Act). Researchers should be able to access and use high-quality datasets, such as patient data, within their fields of activities to create new technological solutions with AI technology, such as AI that processes patient data to prevent and predict diseases. Although, the European health data space will facilitate non-discriminatory access to health data and the training of AI algorithms on those datasets, in a privacy-preserving, secure, timely, transparent, and trustworthy manner, and with appropriate institutional governance (recital 45 Commission's proposed AI Act).[164] Relevant competent authorities, including sectoral ones, providing or supporting access to data may also support the provision of high-quality data for the training, validation, and testing of AI systems (recital 45 Commission's proposed AI Act). Furthermore, the proposed AI Act is designed to intervene only when strictly needed to make it easier for innovation.[165]

Furthermore, recital 72 in the Commission's proposed AI Act removes barriers for Small and Medium Enterprises (SMEs). To address possible disadvantages for SMEs, the proposed AI Act includes several provisions to support SMEs compliance and reduce their costs, including the creation of regulatory sandboxes and obligation to consider SMEs interests when setting fees related to conformity assessment.[166] It is especially important to ensure that SMEs and startups can easily access sandboxes, and are actively involved and participate in the development and testing of innovative AI systems, in order to be able to contribute with their know-how and experience (recital 72 Commission's proposed AI Act). Regulatory sandboxes as such could also be seen as a way to promote innovation, which has already been established in chapter 2.3.3 in this thesis.

[164] See also, European Commission 'Proposal for a regulation of the European Parliament and of the Council on the European Health Data Space' COM(2022) 197 final.

[165] European Commission 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Fostering a European approach to Artificial Intelligence' COM(2021) 205 final, 4.

[166] See 3.3. and 5.2.5 of the Commission's proposed AI Act.

2.4 Summary

There are today many definitions of AI and still no universal definition. This thesis follows the IMCO and LIBE's definition of an AI system in its proposed AI Act. This definition is broad, technology-neutral, and therefore innovation-friendly to AI technology.

AI applications in the first phase, the prevention phase, can affect the rest of the patient journey through early and correct prediction which results in a better-informed patient who can make healthier choices.[167] AI has a comprehensive ability to recognize patterns and identify correlations between data that is hidden in ordinary processing. ML processes large sets of data (Big Data) to find patterns and draw conclusions based on the patterns.[168] With the right training data can the AI system predict diseases and prevent the disease from spreading by deciding the best action plan.[169]

Because AI is a thriving technology it will most likely affect patients' rights.[170] There are challenges with AI technology within healthcare such as the black box effect, transparency, and liability. Access to high-quality data is essential for creating high-performance, robust AI systems.[171] However, a balance between AI innovation and privacy is mandatory to ensure the high quality of the data processed by the AI.

The proposed AI Act has as its general objective to ensure a good functioning single market by establishing conditions for the development and use of safe AI systems. The proposed AI Act lays down harmonized legal rules regarding the development, placement on the EU market, and the use of AI products and services. The specific objectives of the proposed AI Act are to ensure that AI systems placed on the EU market are safe and respect existing EU law and ensure legal certainty to facilitate investment and innovation in AI technology. Furthermore, to enhance governance and effective enforcement of EU law on fundamental rights and safety requirements applicable to AI systems, and lastly, to facilitate the development of a single market for lawful, safe, and trustworthy AI applications and prevent market fragmentation (recital 1 and 5 Commission's proposed AI Act).[172]

[167] Deloitte & MedTech [2020], p. 10.

[168] Kolfschooten [2022], p. 89.

[169] Ibid.; Alpaydin [2020], p. 1.

[170] Kolfschooten [2022], p. 82; Dalton-Brown [2020], p. 115 et seq.

[171] European Commission 'A European approach to artificial intelligence' <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> [Access: 2023-04-06].

[172] European Parliament 'Artificial Intelligence act' [Briefing] (2022), p. 3.

The proposed AI Act follows a risk-based approach which could help to ensure that AI development proceeds safely, responsibly, and in alignment with human values.[173] However, AI systems may jeopardize fundamental rights, like non-discrimination, personal data protection, and privacy.[174] Furthermore, there is a risk that a high-risk approach will prevail and slow down the power of innovation for AI technology within the proposed AI Act.[175]

[173] King [2023].

[174] European Parliament 'Artificial Intelligence act' [Briefing] (2022), p. 2.

[175] Integritetsskyddsmyndigheten [2023], p. 4.

3. Patient Data Protection

3.1 Introduction

This chapter introduces patient data protection. The reader gets an insight into patient data protection as a human- and fundamental right. There is no single EU Bill of Rights. Instead, EU fundamental rights are constructed around art. 6(1) and art. 6(3) of the TEU.[176] Furthermore, the reader gets an insight into patient data protection under data protection regulations, such as the GDPR which is the strongest privacy and security law in the world.[177] It is important for the reader to advance their understanding regarding the legislation behind patient data protection and data privacy. This is important because otherwise, the reader might not fully understand why there is possibly an imbalance between ensuring privacy and promoting innovation in the proposed AI Act. The chapter ends with a summary.

3.2 Regulation for Patient Data Protection

3.2.1 Introduction

There are different legislation regarding patient data protection. This is because patient data protection covers a range of different areas. Such as human rights, fundamental rights, and data protection rights. The term human rights and fundamental rights show overlaps in substance but are of different origins.[178] Fundamental rights are the right of the highest rank in the legal system.[179]

Data Governance Act together with other relevant strategies and acts provides the right base for building high-performance and robust AI systems.[180] Especially regarding patient data protection.

[176] Chalmers, Davies & Monti [2019], p. 252.
[177] European Council 'The general data protection regulation' (2022) <https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/> [Accessed: 2023-05-02].
[178] Janssen [2020], p. 78.
[179] Op. cit., p. 77; See The World Conference on Human Rights 'Vienna Declaration and Programme of Action' (1993).
[180] European Commission 'A European approach to artificial intelligence' <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> [Access: 2023-04-06].

3.2.2 Patient Data Protection as a Human- and Fundamental Right

Art. 8 of the European Charter of Human Rights (ECHR) protects the right to respect private and family life, personal data included.[181] Art. 8 of the CFR is the main vector through which personal data is protected. Art. 8 of the CFR does not mainly concern individuals, but also legal entities.[182] However, not all operations that collect personal data fall within the scope of art. 8 of the CFR.[183] Furthermore, the CFR states in both art. 7 and art. 8 that privacy rights are a fundamental right.[184] The EU legal order is also premised on respect for fundamental rights.[185]

It is up to the EU to ensure that the protection of personal data is followed.[186] The EU has also as its goal to promote the well-being of its people (art. 3 of the TEU). The term well-being is connected to health, thus patient data protection.[187] Furthermore, art. 2 of the TEU states that the Union is founded on the values of respect for human rights.[188] The TEU and the TFEU are essential concerning the EU's power and role regarding patient data protection.

However, the principle of conferral (art. 5(2) TEU) and the principle of subsidiarity (art. 5(3) TEU) could limit the EU's power to protect patients' rights. The principle of conferral limits the EU's power to act only within its competence conferred in the treaties (art. 5(2) TEU). The principle of subsidiarity concerns areas that do not fall within the EU's exclusive competence. The EU shall only act if the proposed action cannot be sufficiently achieved by the Member States (art. 5(3) TEU). A comprehensive legal system for patients rights protection on an EU level does therefore not exist.[189] Healthcare is a national competence and the EU does not have a general competence to take action to protect fundamental rights (art. 168 TFEU).[190]

[181] Pila & Torremans [2019], p. 497; art. 8 of the CFR; Art. 10 of the Convention on Human Rights and Biomedicine.

[182] See Case *Bernh Larsen Holding AS and Others* note 161 (2013); European Court of Human Rights 'Guide to the Case-Law of the European Court of Human Rights' (2022), p. 8.

[183] European Court of Human Rights [2022], p. 9.

[184] World Health Organisation (WHO) & Office of the united nations High Commissioner for Human Rights 'The Right to Health, Fact sheet' <https://www.ohchr.org/sites/default/files/Documents/Publications/Factsheet31.pdf> [Accessed: 2023-04-07], p. 6; see also art. 12 of the Universal Declaration of Human Rights.

[185] Chalmers, Davies, & Monti [2019], p. 251; European Parliament 'Artificial Intelligence act [Briefing] (2022), p. 3 et seq.

[186] See also European Charter of patients' rights, p. 1.

[187] See WHO & Office of the united nations High Commissioner for Human Rights, p. 3.

[188] Chalmers, Davies, & Monti [2019], p. 251.

[189] Kolfschooten [2022], p. 83.

[190] See art. 5(1) of the TEU; Kolfschooten [2022], p. 83; Malu Beijer 'Limits of Fundamental Rights Protection by the EU: The Scope for the Subsidiarity in fundamental rights protection' (2017), Cambridge University Press, p. 179 et seq.

Art. 35 of the CFR explicitly states that a high level of human health protection shall be ensured in the definition and implementation of Union policies and activities.[191] It is further recognized in international human law, more specifically in art. 12 of the International Covenant on Economic, Social, and Cultural Rights that it is a human right to the highest attainable standard of health. A high attainable standard of health could concern the right to information (art. 3 of the European Charter of Patients' Rights (ECPR)). For example, the patient has the right to access all of his/hers patient data. This patient data could include their state of health and all that scientific research and technological innovation make available. All the data and information relative to an individual's state of health, and to the medical/surgical treatments to which he or she is subjected, is considered private and adequately protected (art. 6 ECPR). Furthermore, closely linked to the right to information is the right to consent in art. 3 of the ECPR. However, it could sometimes be difficult to contact the data subject to get valid informed consent (art. 7 GDPR).

The proposed AI Act is based on art. 114 of the TFEU and art. 16 of the TFEU regarding the processing of personal data. Art. 16 of the TFEU provides an appropriate legal basis in cases where the protection of personal data is one of the essential aims/components of the rules adopted by the EU legislature. Furthermore, art. 16 of the TFEU entails the need to ensure independent oversight for compliance with the requirements regarding the processing of personal data, similar to art. 8 of the CFR.[192]

Data quality for building AI-related technologies is of importance for the fundamental rights-compliant use of patient data. Data quality could be defined as whether or not the data used are fit for the purpose. The quality of data depends therefore on the purpose of the use.[193] The quality of the data shall always be non-discriminatory (art. 21 CFR)[194] Non-discrimination is also a fundamental human rights principle and a critical component of the right to health.[195] The International Covenant on Economic, Social, and Cultural Rights identifies the non-exhaustive grounds for discrimination in art. 2(2). These grounds are race,

[191] See also 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; art. 114(3) of the TFEU; See also art. 168(5) of the TFEU which ensures a high level of protection when it comes to health and public health.

[192] 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)' (2021), p. 2.

[193] European Union Agency for Fundamental Rights [2019], p. 11.

[194] European Union Agency for Fundamental Rights [2019], p. 8.

[195] See also art. 11 of the Convention on Human Rights and Biomedicine.

colour, sex, language, religion, political or other opinion, national or social origin, property, disability, birth, or other status.[196] The term other status could cover health status.[197]

Discrimination in the output data could be a result of inadequate input data. Low quality of the input data leads to low quality of the output data (garbage in – garbage out principle) which could violate fundamental rights, thus patient data and privacy.[198]

3.2.3 Patient Data Protection as a Data Protection Right

The GDPR does not explicitly include detailed approaches as to how or at what level of detail fundamental rights impacts should be assessed.[199] Instead, the rights of individuals whose personal data is being processed are at the center of the GDPR.[200] This is because the aim of the GDPR is to give the data subject more control over their personal data.[201] One way of giving the data subject more control is to ensure that personal data are processed in a legal manner (art. 5(1)(a) GDPR). To ensure a legal manner, one of the requirements in art. 6(1) of the GDPR must be fulfilled. Art. 6(3) of the GDPR further states that the legal basis for the processing of personal data shall be regulated in EU law or national law.[202]

The GDPR governs how the personal data of individuals in the EU may be processed and transferred.[203] It is for example not possible to transfer personal data from the EU to a country outside the EU.[204] The definition of personal data is any information relating to an identified or identifiable natural person, also called data subject (art. 4(1) GDPR). An identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier, for example, name, identification number, location data, or online identifier (art. 4(1) GDPR). Every processing of personal data must be underpinned by a legal basis in art. 6 of the GDPR. In the case of Lindqvist, which was about the processing of personal data, the CJEU concluded that personal data covers any operation performed on personal data whether or not automatic means.[205]

[196] See also art. 21 of the CFR.

[197] WHO & Office of the united nations High Commissioner for Human Rights, p. 7.

[198] European Union Agency for Fundamental Rights [2019], p. 2 et seq.

[199] Janssen [2020], p. 85.

[200] European Council 'The general data protection regulation' (2022) <https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/> [Accessed: 2023-05-02]; However, see art. 1(2), art. 35(1) and art. 35(7)(c) of the GDPR. Furthermore, recital 2 & 75 of the GDPR.

[201] Ibid.

[202] See also recital 41 of the GDPR.

[203] European Council 'The general data protection regulation' (2022) <https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/> [Accessed: 2023-05-02].

[204] C-362/14 *Schrems* [EU:C:2015:650]. See also C-311/18 *Facebook Ireland and Schrems* [EU:C:2020:559].

[205] C-101/01 *Bodil Lindqvist v. Åklagarkammaren* [EU:C:2003:596].

There are special categories of personal data, such as data concerning health (art. 9 GDPR). Data concerning health is 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 (art. 4(15) GDPR).[206] Data regarding health is covered by sensitive data and processing of sensitive data is prohibited (art. 9(1) GDPR). However, there are three (3) exceptions in art. 9(2) of the GDPR. Firstly, the processing of sensitive personal data, such as patient data, may be accepted if it is necessary for reasons related to, prevention and the provision of health care (art. 9(2)(h) GDPR). A potential argument regarding AI could be that it is necessary for the AI system to be trained with patient data in order to prevent and predict diseases.[207] Secondly, the processing of sensitive personal data must comply with EU law or national law or comply with agreements with professionals in the health field. Such as the CFR and the ECHR. Thirdly, the conditions and the protective measures in art. 9(3) of the GDPR must be fulfilled.[208] These protective measures are that the data shall be processed by or under the responsibility of a professional subject to the obligation of professional secrecy.

How about anonymous data? Anonymous data is not covered by the GDPR because it can not be traced back to an individual (recital 26 GDPR). However, anonymizing all of the large datasets of patient data is practically impossible. There is always a risk of re-identification of individuals regarding medical records which could harm the data subject's private life.[209]

GDPR demands clarity, precision, predictability, and proportionality regarding the processing of personal data (art. 6(3) GDPR).[210] The GDPR is subject to the proportionality principle regarding the processing of personal data (art. 5(4) TEU). The proportionality principle aims at the action which shall not exceed what is necessary to achieve the objectives of the Treaties (art. 5(4) TEU).[211] For example, patient data that has been collected by an AI system shall be proportionate regarding the purpose to prevent and predict diseases. A company can therefore not collect more patient data than necessary for its goal. Thus, the collected data has to be necessary (art. 6(1)(e) GDPR). The requirement of necessity shall be interpreted together with the principle of data minimization (art. 5(1)(c) GDPR). The principle of minimization establishes that collection of personal data must be adequate, relevant, and not too extensive

[206] See also art. 3 of the CFR; recital 35 of the GDPR.
[207] Integritetsskyddsmyndigheten [2023], p. 15.
[208] Integritetsskyddsmyndigheten [2023], p. 12.
[209] Kolfschooten [2022], p. 97; Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye 'Estimating the success of re-identifications in incomplete datasets using generative models' (2019), Nature Communications, p. 3069.
[210] See also recital 41 of the GDPR.
[211] C-508/13 *Estonia v. Parliament and Council* EU:C:2004:443.

in relation to the purpose for which they are processed (art. 5(1)(c) GDPR). The degree of clarity and precision required is decided on a case-by-case basis.[212] The principle of minimization can seem meaningless in the context of AI because the training of the AI algorithm requires enormous datasets (art. 5 GDPR).

Regarding predictability, the data subjects' access to information is stated in the art. 13(2)(f) and art. 14(2)(g) of the GDPR. These articles refer to information that has to be provided to data subjects. Art. 15(1)(h) of the GDPR refers to the obligation to provide data subjects with meaningful information about the logic involved and with the significance and the envisaged consequences of the processing.[213] The data subject should therefore always have the right of access to personal data which have been collected concerning him or her (recital 63 GDPR).[214] The data subject has also the right to withdraw consent (art. 7(3) GDPR).

Furthermore, if a data subject wishes, it has the right of erasure. The right of erasure was put into practice in the case of Google Spain and Google.[215] In the case of Google Spain, the main concern was the need to ensure a correct balance between the data subject's protection of personal data and respect for privacy and the public's interest in being informed. The CJEU shared that application of fundamental rights should be based on an optimal assessment of the various interests at stake (art. 7-8 CFR).[216]

The data subject shall have the right not to be subject to a decision that may include a measure, evaluating personal aspects relating to the data subject which is based solely on automated processing and which produces legal effects concerning the data subject, also called profiling (recital 71 and art. 22 GDPR).[217] To protect this right the controller shall implement measures. The controller is a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (art. 4(7) GDPR). However, there are two (2) exceptions from this right. One (1), if it's necessary, authorized by European Union or Member State law, or two (2) if the subject's explicit consent. Furthermore, the data controllers shall also provide meaningful information regarding processing for the data subject.[218]

[212] See Integritetsskyddsmyndigheten [2023], p. 10 et seq.
[213] Kolfschooten [2022], p. 89.
[214] The data subject's right to access is further stated in art. 16, 17, and 21 of the GDPR.
[215] C-131/12 *Google Spain and Google* EU:C:2014:317.
[216] C-131/12 *Google Spain*; Gregorio & Dunn [2022], p. 495 et seq.
[217] See the definition of profiling in art. 4(4) of the GDPR.
[218] European Union Agency for Fundamental Rights [2019], p. 10.

Additionally, it is a principle of data accuracy in the GDPR, which is related to data quality. The principle of data accuracy in the GDPR is shown in a very narrow sense because it only focuses on the obligation to keep personal data accurate and up to date.[219] Regarding AI-related technologies, data quality meant much wider. To ensure high data quality regarding AI-related technologies, a clear data protection law is needed. When assessing the quality of data for AI applications, many criteria can be taken into consideration. Data quality includes many different issues such as completeness, accuracy, consistency, timeliness, duplication, validity, availability, and provenance.[220]

Furthermore, except the GDPR, the Convention for the Protection of Individuals with regard to the automatic processing of personal data, also called Convention 108, is relevant regarding patient data processing (art. 1 Convention 108). The EU Member States have all signed up for Convention 108. This Convention protects for example the patient against abuses of collection and processing of their personal data. The Convention also regulates the transborder flow of personal data.[221] Personal data is defined as any information relating to an identified or identifiable individual (art. 2 Convention 108).[222] Moreover, Convention 108 states that sensitive data, such as data concerning health, are not to be processed in the absence of proper legal safeguards. However, a balance between other interests than personal data protection is needed and the Convention 108 can be overridden by for example public safety.[223] Public safety could for example have been referred to during the COVID-19 pandemic.

Concerning AI technology within healthcare, MDR is mainly the regulation at the EU level regarding health technology.[224] However, MDR regulates and ensures the quality of medical devices rather than patients' rights. AI technology could qualify as a medical device and therefore be subject to MDR.[225] The definition of a medical device is stated in the art. 2(1) of the MDR and can be software for medical purposes such as the prevention and prediction of diseases.[226] MDR protects privacy and data protection by referring to the GDPR, MDR does

[219] European Union Agency for Fundamental Rights [2019], p. 9.
[220] Op. cit., p. 10.
[221] Pila & Torremans [2019], p. 498.
[222] European Court of Human Rights [2022], p. 7.
[223] Pila & Torremans [2019], p. 498.
[224] Kolfschooten [2022], p. 88; 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/EEC (Text with EEA relevance.)
[225] Kolfschooten [2022], p. 102.
[226] Exclusions are found in recital 19 of the MDR.

not add requirements in that way (art. 109-110 MDR).[227] Future medical AI tools should fulfill all the requirements in the MDR.[228]

3.3 Summary

Patient rights have clear roots in the notion of human dignity, ethical principles, and human rights standards.[229] It is clear that patients' rights are threatened when health AI is used. Lack of protection of sensitive personal data such as patient data may cause distrust in health AI.[230] AI technology processes, collects, and analyzes the data subject's personal data which could affect the data subject's right to medical data protection and privacy.[231]

Fundamental rights offer a solid base of protection regarding the processing of personal data. Furthermore, the GDPR offers broad protection for patient data protection (art. 4(13-15) and art. 9 GDPR).[232] The GDPR offers broad protection because the dignity of the human person and privacy are important aspects of the GDPR.[233] For example, personal data shall always be processed lawfully, fairly, and in a transparent manner vis-a-vis the data subject. Personal data can only be collected for a specific, explicit, and legitimate purpose. Furthermore, data collection needs to be proportional, as it needs to be adequate, relevant, and necessary in relation to the purpose of the exercise.[234] The lawfulness of the reuse of patient data depends on the compatibility among the purposes for which the data are further processed.[235]

Moreover, Convention 108 and the MDR are also relevant legislation regarding patient data protection and AI technology that processes patient data. However, the protection of patient data is not absolute, a balance between other interests and rights is needed.[236]

[227] See also Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety regarding health.
[228] European Parliament 'Artificial intelligence in healthcare - Applications, risks, and ethical and societal impacts' (2022), EPRS, p. 32.
[229] Kolfschooten [2022], p. 84; Cohen & Ezer [2013].
[230] Kolfschooten [2022], p. 95; European Union Agency for Cybersecurity [2020].
[231] Kolfschooten [2022], p. 97; Daelman [2021], p. 126 et seq.
[232] See also recital 51-56 of the GDPR.
[233] Ciancimino [2022], p. 174; see also Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, officers and agencies and on the free movement of such datam and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.
[234] Pila & Torremans [2019], p. 503.
[235] Ciancimino [2022], p. 176.
[236] Pila & Torremans [2019], p. 498.

4. A Balance Between Innovation and Privacy in the Proposed AI Act?

4.1 Introduction

This chapter analyzes if there is a balance in the proposed AI Act regarding promoting innovation and ensuring privacy concerning the collection of patient data for the prevention and prediction of diseases. The term balance is to be interpreted in this thesis as weighing scales. One scale pan may weigh more, but the balance is considered disturbed if one scale pan tips over.[237] It would therefore be optimal to find solutions regarding ensuring privacy without hindering innovation.

There are different opinions regarding how the proposed AI Act promotes innovation and ensures privacy. This chapter will therefore describe criticism regarding both the aspect of promoting innovation and ensuring privacy in the proposed AI Act. Differences concerning promoting innovation and ensuring privacy regarding the collection of patient data for the prevention and prediction of diseases in the three (3) proposed AI Acts will also be addressed. This chapter ends with a summary.

4.2 Does the Proposed AI Act Ensure Privacy and Promote Innovation with Regard to the Collection of Patient Data?

4.2.1 Introduction

The proposed AI Act aims to both protect fundamental rights, such as data privacy, and promote innovation. The Proposed AI Act has however been criticized for not balancing these two (2) aspects.[238] It could for example be seen as no surprise that chapter 2.3.3 which is about ensuring data privacy in this thesis is more extensive than chapter 2.3.4 regarding promoting innovation.

[237] The word harmony could possibly also be used.

[238] Kolfschooten [2022], p. 106; Algorithm Watch 'AlgorithmWatch's response to the European Commission's proposed regulation on Artificial Intelligence - A major step with major gaps' (2021) <https://algorithmwatch.org/en/response-to-eu-ai-regulation-proposal-2021/> [Accessed: 2023-04-11].

4.2.2 Criticism Regarding Ensuring Privacy

The Commission's proposal for an AI Act according to Kolfschooten lacks a human-centered approach. The proposal does not for example include the end users such as patients. Instead, the proposal focuses on companies.[239] To see patients as sources of data and not as human beings threaten the notion of human dignity.[240] The Rapporteur of the Committee on the Environment, Public Health and Food Safety shares Kolfschooten's approach in their opinion regarding extending the scope to end users because it is especially important in healthcare.[241]

The OECD also addresses the importance of human-centered values and fairness. AI actors should respect the rule of law and human rights. These include privacy and data protection.[242] Transparency and explainability are something AI actors should commit to.[243] However, the IMCO and LIBE's proposal for an AI Act addresses the importance of a human-centric approach regarding AI technology in recital 4(a) in their proposed AI Act.

Furthermore, the right to informed consent may also be threatened because the end user, in this case, the patient is not prioritized.[244] The first cornerstone of the data subjects' rights is according to Pila and Torremans the requirement for greater transparency.[245] AI systems should be robust, secure, and sage throughout their entire lifecycle.[246] It could be argued that transparency right is not that useful due to the algorithm of the AI being hard to understand for a patient.[247] The opinion of the European Committee of the Regions shares Pila and Torreman's opinions regarding greater transparency.[248] The transparency and information requirements applicable to providers and users should be extended to the persons or groups of persons potentially affected by the use of high-risk AI. Recital 47 in the Commission's proposed AI Act should change from a *certain degree* to a *high degree* of transparency. The Council and IMCO and LIBE have not addressed this issue in their AI Act proposals.

[239] Kolfschooten [2022], p. 106.
[240] Op. cit., p. 109; Evelyne Shuster 'Fifty years later: The significance of the Nuremberg Code' (1997), Nejm, p. 1436 et seq.
[241] Committee on the Environment, Public Health and Food Safety for the Committee on the Internal Market and Consmer Protection and for the Committee on Civil Liberties, Justice and Home Affairs on 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 (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD)) [opinion] (2022), p. 4.
[242] See 1.2. in the OECD Recommendation of the Council on Artificial Intelligence.
[243] See 1.3. in the OECD Recommendation of the Council on Artificial Intelligence.
[244] Kolfschooten [2022], p. 109; Shuster [1997], p. 1436 et seq.
[245] Pila & Torremans [2019], p. 507.
[246] See 1.4. in the OECD Recommendation of the Council on Artificial Intelligence.
[247] Kolfschooten [2022], p. 101.
[248] European Committee of the Regions - European approach to artificial intelligence - Artificial Intelligence Act (COM(2021)206) [opinion] (2021).

More transparency is certainly needed regarding regulatory sandboxes.[249] Regulatory sandboxes have a double role, they foster business learning, such as the development and testing of innovations in a real-world environment and it also supports regulatory learning, such as the formulation of experimental legal regimes to guide and support businesses in their innovation activities under the supervision of a regulatory authority.[250] Regulatory sandboxes have emerged as testbeds in health, for example for services and innovations for predictive and early detection of diseases.[251]

The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) recommend a clarification of the scope and objectives regarding regulatory sandboxes. Furthermore, the Commission's proposed AI Act should also clarify that sandboxes should comply with the requirements in existing data protection frameworks. The EDPB and the EDPS state that a clear relation between the certification system and the EU data protection law is missing. The IMCO and LIBE proposal for an AI Act makes this relation more clear (recital 72(a) IMCO and LIBE proposed AI Act).

The EDPB and the EDPS see it also as problematic regarding AI technology that further processes data. This is not adequately regulated. For example, art. 54 of the Commission's proposed AI Act does not address two important issues, (1) under what circumstances, using which criteria are the interests of data subjects weighed, (2) whether these AI systems will only be used within the regulatory sandbox.[252] Furthermore, to avoid any inconsistency and possible conflict with the GDPR. Clarification on the further processing of personal data for developing certain AI systems and the re-use of personal data is therefore needed.[253] This is amended in art. 54 in the IMCO and LIBE proposed AI Act.

Moreover, the Commission's proposed AI Act does not take into consideration the principle of data minimization and data protection by design. The EDPB and the EDPS recommend clarifying the relationship between certificates issued in the proposed AI Act and data protection certifications, seals, and marks.[254] The IMCO and LIBE proposal of an AI Act takes this into consideration in recital 45(a) of their proposed AI Act. The Council's proposal

[249] European Parliament 'Artificial intelligence act and regulatory sandboxes'[briefing] (2022).
[250] Op. cit., p. 2.
[251] Ibid.
[252] Ibid.
[253] European Parliament 'Artificial intelligence act and regulatory sandboxes'[briefing] (2022), p. 2.
[254] EDPB & EDPS [2021] p. 3.

of an AI Act takes data minimization into consideration (recital 44(a) Council's proposed AI Act) but not data protection by design.

The EDPB and the EDPS continue their criticism of the code of conduct. It is important to clarify if the protection of personal data is to be considered among *additional requirements* that can be addressed by these codes of conduct, and to ensure that the *technical specifications and solutions* do not conflict with the rules and principles of the existing EU data protection framework.[255] This is not further addressed in the Council's or the IMCO and LIBE's proposals for an AI Act.

Amendments shall be made regarding the Commission's proposed AI Act risked-based approach. Academics fear that the Commission's proposed AI Act would not ensure a high level of protection of fundamental rights. The Commission's proposal of an AI act does not always establish accurate wrongs and harms associated with different kinds of AI systems and therefore does not appropriately allocate responsibility. Galaz recommends the Commission broaden the lift of prohibited AI systems and ban existing manipulative AI systems. Eber and others promote more details regarding the classification of risks and prohibit more AI systems.[256] However, this is included in recitals 33 and 35 in the IMCO and LIBE proposals of an AI Act. The Council also includes this in their proposal (art. 4 Council's proposed AI Act).

Lastly, the Commission's proposed AI Act has been criticized for lack of adequate remedies.[257] This per se affects data privacy. The IMCO and LIBE proposal of an AI Act does however clarify remedies in recital 84(b).

4.2.3 Criticism Regarding Promoting Innovation

The proposed AI Act has a strong focus on ensuring privacy which could affect innovation negatively. The proposed AI Act has been criticized for its potential added costs in compliance, which could cold down investors and hinder start-ups.[258] The proposed AI Act

[255] EDPB & EDPS [2021] p. 3.

[256] See Victor Galaz (et al) 'Artificial intelligence, systemic risks, and sustainability' (2021), Technology in Society; European Parliament 'Artificial Intelligence act [Briefing] (2022), p. 9 et seq.

[257] Gregorio & Dunn [2022], p. 492.

[258] Ali Spina & Yu [2021], p .25; Benjamin Mueller 'How Much Will the Artificial Intelligence Act Cost Europe?' (2021) <https://datainnovation.org/2021/07/how-much-will-the-artificial-intelligence-act-cost-europe/> [Accessed: 2023-05-07]; Benjamin Mueller 'The Artificial Intelligence Act is a Threat to Europe's Digital Economy and Will Hamstring the EU's Technology Sector in the Global Marketplace' (2021) <https://datainnovation.org/2021/04/the-artificial-intelligence-act-is-a-threat-to-europes-digital-economy-and-will-hamstring-the-eus-technology-sector-in-the-global-marketplace/> [Accessed: 2023-05-07].

will cost the European economy €31 billion over the next five (5) years and as a result, reduce AI investments by almost 20 percent.[259] If the current proposed AI Act is adopted, it will be the world's most restrictive regulation of the development and use of AI tools.[260] However, the estimations of the compliance costs for the proposed AI Act are challenged by inter alia economists.[261]

Furthermore, the newly adopted Recovery and Resilience Facility (RRF) will support reforms and investments by Member States for the crucial first years of the recovery. At least 20% of the available funding will be allocated to measures fostering the digital transition. The RRF could boost investments from the Member States to support research, innovation, and testing capacities regarding AI. The RRF could help to accelerate the development and use of AI and contribute to economic and social recovery and improve competitiveness in the longer term.[262]

Mueller describes that the Commission's proposed AI Act has a chilling effect on innovation because the definition of AI is too broad and covers any software using ML techniques (art. 3 Commission's proposed AI Act).[263] It has been suggested to narrow the definition of an AI system.[264] The Council's and IMCO and LIBE's definition of an AI system has in that sense a narrower scope. Furthermore, the Commission's proposal for an AI Act did not contain any specific provision regarding general-purpose AI technologies. The Council's proposed AI Act includes that specific provisions regarding general-purpose AI technologies should be considered.[265]

The EDPB and the EDPS highlight the risk of an exhaustive list of high-risk AI systems. It could create weak attraction capabilities in highly risky situations. Furthermore, the list of high-risk AI systems in Annex II and Annex III in the Commission's proposed AI Act lacks some types of use cases that involve significant risks. For example, the use of AI for assessing medical treatments or for health research purposes. The EDPB and the EDPS want to see an

[259] Benjamin Mueller 'How Much Will the Artificial Intelligence Act Cost Europe?' (2021) <https://datainnovation.org/2021/07/how-much-will-the-artificial-intelligence-act-cost-europe/> [Accessed: 2023-05-07].

[260] Ibid.

[261] European Parliament 'Artificial Intelligence act [Briefing] (2022), p. 9.

[262] Commission 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Fostering a European approach to Artificial Intelligence' COM(2021) 205 final, p. 2.

[263] Benjamin Mueller 'The Artificial Intelligence Act is a Threat to Europe's Digital Economy and Will Hamstring the EU's Technology Sector in the Global Marketplace' (2021) <https://datainnovation.org/2021/04/the-artificial-intelligence-act-is-a-threat-to-europes-digital-economy-and-will-hamstring-the-eus-technology-sector-in-the-global-marketplace/> [Accessed: 2023-05-07].

[264] European Parliament 'Artificial Intelligence act [Briefing] (2022), p. 8.

[265] European Parliament 'General-purpose artificial intelligence' (2023).

update to ensure that the scope in Annex II and Annex III is appropriate.[266] An update in the annexes has especially been done in the IMCO and LIBE proposal of an AI Act and covers a more broad scope.

The proposed AI Act focuses too much on potential threats rather than actual threats such as surveillance, disinformation, or social control. This could reduce the use of many socially beneficial applications of AI systems. Muelles promotes a light-touch framework limited in scope and adapts it based on observed harms.[267] Moreover, the Commission's proposed AI Act prescribes an overly strict transparency regime for the information submitted during the conformity assessment of AI technology. More concretely, the proposed AI Act treats all the submitted information as confidential information and allows disclosure only between public authorities.[268]

The Rapporteur of the Committee on Industry, Research and Energy believes SMEs and start-ups should be more involved throughout the proposed AI Act in a holistic approach (art. 55 Commission's proposed AI Act).[269] Amendments are especially needed in recitals 72 and 73 of the Commission's proposed AI Act. The suggested amendment is to give SMEs and start-ups more space within the proposed AI Act. The European Digital SME Alliance shares this approach and adds that sandboxes should be mandatory in all EU Member States.[270] This is also stressed in the Council and the IMCO and LIBE proposals for an AI Act.

As previously stated, regulatory sandboxes will not exclude participation from liability (art. 53(4) Commission's proposed AI Act). Some authors stress that regulatory sandboxes would be used for ensuring innovative products are compliant with current regulations. However, regulatory sandboxes would not serve for assessing the AI innovation's exposure to potential liability. Regulatory sandboxes could make participants in an AI sandbox expose their trade secrets. The proposed AI Act is not clear regarding regulatory relief for innovators. It would be a good idea to clarify the liability protection benefits in the sandbox.[271] Furthermore,

[266] EDPB & EDPS [2021], p. 9.
[267] Benjamin Mueller 'The Artificial Intelligence Act is a Threat to Europe's Digital Economy and Will Hamstring the EU's Technology Sector in the Global Marketplace' (2021) <https://datainnovation.org/2021/04/the-artificial-intelligence-act-is-a-threat-to-europes-digital-economy-and-will-hamstring-the-eus-technology-sector-in-the-global-marketplace/> [Accessed: 2023-05-07].
[268] Ali Spina & Yu [2021], p. 25.
[269] Committee on Industry, Research and Energy for the Committee on the Internal Market and Consumers Protection and the Committee on Civil Liberties, Justice and home Affairs on 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 (COM(2021)0206-C9-0146/2021 - 2021/0106(COD)) [opinion] (2022).
[270] European Parliament 'Artificial Intelligence act [Briefing] (2022), p. 9.
[271] European Parliament 'Artificial intelligence act and regulatory sandboxes' [briefing] (2022), p. 2.

regulatory sandboxes are optional and not mandatory for Member States. Different sandbox frameworks and rules could be implemented as a result of the optionality. The risk is having diverging national sandboxing rules.[272] This is however also stressed in the Council and the IMCO and LIBE proposals for an AI Act.

4.3 Summary

The proposed AI Act aims to find a balance between promoting innovation and ensuring privacy. However, this balance seems difficult to establish. The proposal has been criticized regarding its high-risk approach and strong protection regarding safe AI.

Before AI systems can be used in the EU, the proposed AI Act contains rules to enhance transparency and minimize risks to safety and fundamental rights.[273] However, there are concerns both regarding if patient data and privacy as a fundamental right are enough protected and if transparency hinders innovation within health.

The proposed AI Act as a whole creates a proportionate and risk-based European regulation. For example, the proposed AI act provides a technology-neutral and future-proof definition of AI systems. The proposed definition covers techniques that are not yet known or developed.[274] The definition in the proposed AI Act has been criticized to be too extensive and too restrictive. Furthermore, the proposed AI Act focuses on high-risk AI use cases to avoid regulatory overreach. The intended purpose of the system and the severity of possible harm and the probability of the harm to occur decides if the AI system shall be classified as high-risk. Use cases make it possible to create a future-proof AI Act which could classify new AI systems as high-risk within certain predefined areas of use.[275] However, some people see this as problematic regarding certainty in the legislation.

It has especially been an extensive discussion about regulatory sandboxes and SMEs. As no surprise, there are different opinions regarding if the information in the different proposals is enough for regulatory sandboxes and SME exceptions.

[272] European Parliament 'Artificial intelligence act and regulatory sandboxes' [briefing] (2022), p. 2.

[273] Commission 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Fostering a European approach to Artificial Intelligence' COM(2021) 205 final, p. 4.

[274] Ibid.

[275] Ibid.

Lastly, AI systems of high risk need to comply with specifically designed requirements. These requirements include high-quality datasets, the establishment of appropriate documentation to enhance traceability, the sharing of adequate information with the user, the design and implementation of appropriate human oversight measures, and the achievement of the highest standards in terms of robustness, safety, cybersecurity, and accuracy. Many concerns here are especially on the innovation aspect. There are high requirements that high-risk AI systems must comply with before being placed on the market or put into service.[276]

[276] Commission 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Fostering a European approach to Artificial Intelligence' COM(2021) 205 final, p. 4.

5. Summary and Conclusions

In recent years the use of AI in medicine and healthcare has been praised for the free promise it offers but has also been at the center of heated controversy. For example, AI technology could improve medical diagnosis and treatment. The AI technology could also include risk of bias and increased health inequalities, lack of transparency and trust, and vulnerability to hacking and data privacy breaches. It is unclear if the current EU framework for patients' rights is sufficient regarding innovative technology.[277] Therefore the proposed AI Act was created.

AI is a rapidly developing family of technologies that require regulatory oversight and a safe and controlled space for experimentation. At the same time ensuring responsible innovation and integration of appropriate safeguards and risk mitigation measures (recital 71 Commission's proposed AI Act). The proposed AI Act seeks therefore to create an environment where AI technology is developed and where EU values and fundamental rights are protected. The proposed AI Act is aware of the potential development regarding AI technology and at the same time, aware of the threats such as black box and cyberattacks.[278] However, the proposed AI Act could be seen to not fulfill this purpose.

The proposed AI Act does ensure privacy with regard to the collection of patient data for the prevention and prediction of diseases by its risk-based approach. AI within health could for example be considered as a high-risk AI system. Furthermore, the proposed AI Act promotes innovation with regard to the collection of patient data for the prevention and prediction of diseases by research exceptions, regulatory sandboxes, and lowering the barrier for SMEs.

However, a balance between innovation and privacy in the proposed AI Act with regard to the collection of patient data for the prevention and prediction of diseases is not quite fulfilled. On the one hand, the proposed AI Act hinders innovation because of its strict focus on ensuring patient data protection and privacy. The proposed AI Act includes for example more recitals and articles on ensuring privacy compared to recitals and articles on promoting innovation within healthcare. This was, in my opinion, expected because there is already

[277] Kolfschooten [2022], p. 82.

[278] Gregorio & Dunn [2022], p. 494; Commission 'Shaping Europe's digital future' (communication) COM(2020)67 final.

existing legislation that ensures data privacy and patient data protection. Such as the CFR, ECHR, and the GDPR. Furthermore, regarding cybersecurity and trust in AI systems is it also a smart idea to be more on the safe side. People and businesses should be able to enjoy the benefits of AI and feel safe and protected.

What is my educated guess regarding the proposed AI Act? I think the proposed AI Act will take a more protective approach than an innovative approach. I also think that the finished regulation will be a combination of the three (3) proposals of an AI Act. Regarding the definition of an AI system, my educated guess is that it can be either one of the suggestions or something completely different. However, it will be interesting to see later this year what the AI Act will look like!

Bibliography

Official Publications

European Union

European Parliament 'Artificial intelligence in healthcare - Applications, risks, and ethical and societal impacts' (2022), EPRS.

European Council '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' (General approach) (2022).

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' COM(2021) 206 final.

European Commission 'Proposal for a regulation of the European Parliament and of the Council on the European Health Data Space' COM(2022) 197 final.

European Commission 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Single Market Strategy for Europe' COM(2015) 192 final.

European Commission 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Shaping Europe's digital future' COM(2020) 67 final.

European Commission 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Fostering a European approach to Artificial Intelligence' COM(2021) 205 final.

European Commission 'White Paper On Artificial Intelligence – A European approach to excellence and trust' COM(2020) 65 final.

Committee on the Internal Market and Consumer Protection & Committee on Civil Liberties & Justice and Home Affairs 'Draft Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonised rules on

Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts' (2023).

Committee on the Environment, Public Health and Food Safety for the Committee on the Internal Market and Consmer Protection and for the Committee on Civil Liberties, Justice and Home Affairs 'Opinion on 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 (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD)).

Committee on Industry, Research and Energy for the Committee on the Internal Market and Consumers Protection and the Committee on Civil Liberties, Justice and home Affairs 'Opinion on 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 (COM(2021)0206-C9-0146/2021 - 2021/0106(COD)).

European Data Protection Board & European Data Protection Supervisor '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)' (2021).

High-Level Expert Group on Artificial Intelligence 'Ethics Guidelines for Trustworthy AI' (2019), Commission.

High-Level Expert Group on Artificial Intelligence 'A definition of AI: Main capabilities and disciplines - Definition developed for the purpose of the deliverables of the High-Level Expert Group on AI' (2018), Commission.

Literature

Alder S 'AI Company Exposed 2.5 Million Patient Records Over the Internet' (2020), HIPPA Journal.

AL-Hashimi M & Hamdan A, *Artificial Intelligence and Coronavirus COVID-19: Applications, Impact and Future Implications* in The Importance of New Technologies and Entrepreneurship in Business Development: In The Context of Economic Diversity in Developing Countries (ResearchGate 2021).

Ali Spina G & Yu R, '*Artificial Intelligence between Transparency and Secrecy: From the EC Whitepaper to the AIA and Beyond'* (2021), EJLT.

Alpaydin E, *Introduction to Machine Learning* (MIT Press 2020).

Bathaee Y 'The artificial intelligence black box and the failure of intent and causation' (2018), Harvard Journal of Law & Technology.

Beijer M 'Limits of Fundamental Rights Protection by the EU: The Scope for the Subsidiarity in fundamental rights protection' (2017), Cambridge University Press.

Chalmers D, Davies G & Monti G, *European Union Law* (Cambridge University Press 2019).

Christensen K 'Exhibiting transparency without opening the 'Black Box' - Balancing act between Data Protection and Trade Secrets Rights in Solely Automated Decision-Making AI system in Healthcare' (2020), Lund University.

Ciancimino M 'AI-Based Decision-Making Process in Healthcare - Towards a More Consistent Processing of Personal Data' (2022), EuCML.

Cohen J & Ezer T 'Human rights in patient care: A theoretical and practical framework' (2013), Health and Human Rights Journal.

Daelman C 'AI through a human rights lens. The role of human rights in fulfilling AI's potential' (2021), Artificial Intelligence and the Law.

Dalton-Brown S 'The ethics of medical AI and the physician-patient relationship' (2020), Cambridge Quarterly of Healthcare Ethics.

Davenport T & Kalakota R, *The potential for Artificial intelligence in healthcare* (Future Healthcare Journal 2019).

Deloitte & MedTech Europe 'The socio-economic impact of AI in healthcare' (2020), Deloitte.

Ekdal D 'Normative Power Europe & AI: How the EU intends to normatively govern artificial intelligence technologies through the Artificial Intelligence Act and its "trustworthy" and "human-centric" approach' (2021), Lund University.

European Court of Human Rights ‘Guide to the Case-Law of the European Court of Human Rights’ (2022).

European Parliament ‘General-purpose artificial intelligence’ (2023).

European Parliament ‘Artificial Intelligence act’ (Briefing) (2022).

European Parliament ‘Artificial intelligence act and regulatory sandboxes’ (briefing) (2022).

European Union Agency for Cybersecurity ‘Artificial Intelligence Cybersecurity Challenges. Threat Landscape for Artificial Intelligence’ (2020).

European Union Agency for Fundamental Rights ‘Data quality and artificial intelligence: mitigating bias and error to protect fundamental Rights’ (2019), FRA.

Galaz V (et al) ‘Artificial intelligence, systemic risks, and sustainability’ (2021), Technology in Society.

Gerke S, Minssen T & Cohen G ‘Ethical and legal challenges of artificial intelligence-driven healthcare’ (2020), Academic Press.

Gregorio G & Dunn P ‘The European Risk-based Approaches: Connecting Constitutional Dots in the Digital Age’ (2022), Common Market Law Review.

Gunnarsson Å & Svensson E *Rättsdogmatik: som rättsvetenskapligt perspektiv och metod* (Studentlitteratur 2023).

Hellner J, *Metodproblem i rättsvetenskapen. Studier i förmögenhetsrätt* (Jure 2001).

Hettne J & Eriksson O (ed.), *EU-rättslig metod: teori och genomslag i svensk rättstillämpning* (Norstedts juridik 2011).

Integritetsskyddsmyndigheten ‘Federerad maskininlärning mellan två vårdgivare - Slutrapport om Integritetsskyddsmyndighetens pilotprojekt med regulatorisk testverksamhet om dataskydd’ (2023), IMY.

Janssen H ‘An approach for a fundamental rights impact assessment to automated decision-making’ (2020), International Data Privacy Law.

Jareborg N ‘Rättsdogmatik som vetenskap’ (2004), SvJT.

King C ‘Exploring the Precautionary Principle in AI Development: Historical Analogies and Lessons Learned’ (2023), Lesswrong.

Kolfschooten H, *EU regulation of artificial intelligence: Challenges for patients’ rights* (Common Market Law Review 2022).

Malina D (ed) ‘Hidden in Plain Sight — Reconsidering the Use of Race Correction in Clinical Algorithms’ (2020), The New England Journal of Medicine.

Matheny M, Israni S, Ahmed M & Whicher D, *Artificial Intelligence in Health Care: The Hope, the Hype, the Promise, the Peril* (National Academy of Medicine 2019).

McCall B, *COVID-19 and artificial intelligence: Protecting health-care workers and curbing the spread* (Lancet Digital Health 2020).

McKeown A, Mourby M, Harrison P, Walker S, Sheehan M & Singh I ‘Ethical issues in consent for the reuse of data in health data platforms’(2021), Science and Engineering Ethics.

Nääv M & Zamboni M, *Juridisk metodlära* (Studentlitteratur 2018).

OECD ‘Recommendation of the Council on Artificial Intelligence’ (2019).

Peczenik A, *Juridikens teori och metod* (Norstedts juridik 1995).

Pickering B ‘Trust, but Verify: Informed Consent, AI Technologies, and Public Health Emergencies, Future Internet’ (2021), MDPI.

Pila J & Torremans P, *European Intellectual Property Law* (Oxford University Press 2019).

Ploug T & Holm S ‘Meta Consent –A Flexible Solution to the Problem of Secondary Use of Health Data’ (2016), Bioethics.

Price II Nicholson W ‘Regulating black-box medicine’ (2017), Michigan Law Review.

Rashid J, Batool S, Kim J, Wasif Nisar M, Hussain A, Juneja S & Kushwaha R ‘An Augmented Artificial Intelligence Approach for Chronic Diseases Prediction’ (2022), Frontiers in Public Health.

Rocher L, Hendrickx J & Montjoye Y ‘Estimating the success of re-identifications in incomplete datasets using generative models’ (2019), Nature Communications.

Shuster E ‘Fifty years later: The significance of the Nuremberg Code’ (1997), Nejm.

Strömholm S, Lyles M & Valguarnera F, *Rätt, rättskällor och rättstillämpning. En lärobok i allmän rättslära* (Nordstedts Juridik 2020).

Zapusek T ‘Artificial intelligence in medicine and confidentiality of data’ (2017), Asia Pacific Journal of Health Law and Ethics.

Österman E ‘Legal Regulation for Artificial Intelligence in the European Union - Major Aspects for Minor’ (2022), Lund University.

Online sources

Algorithm Watch ‘AlgorithmWatch’s response to the European Commission’s proposed regulation on Artificial Intelligence - A major step with major gaps’ (2021) <https://algorithmwatch.org/en/response-to-eu-ai-regulation-proposal-2021/> [Accessed: 2023-04-11].

BBC ‘Google DeepMind NHS app test broke UK privacy law’ (2017) <https://www.bbc.com/news/technology-40483202> [Accessed: 2023-05-15].

Bertuzzi L ‘AI Act moves ahead in EU Parliament with key committee vote’ (2023) <https://www.euractiv.com/section/artificial-intelligence/news/ai-act-moves-ahead-in-eu-parliament-with-key-committee-vote/> [Accessed: 2023-05-11].

Bertuzzi L ‘AI Act: European Parliament headed for key committee vote at end of April’ (2023) <https://www.euractiv.com/section/artificial-intelligence/news/ai-act-european-parliament-headed-for-key-committee-vote-at-end-of-april/> [Accessed: 2023-04-25].

European Commission ‘A European approach to artificial intelligence’ <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> [Accessed: 2023-04-06].

European Commission ‘Ethics Guidelines for Trustworthy AI’ (2019) <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> [Accessed: 2023-04-29].

European Council ‘Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights’ (2022) <https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/> [Accessed: 2023-04-07].

European Council ‘The general data protection regulation’ (2022) <https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/> [Accessed: 2023-05-02].

European Parliament ‘AI Act: a step closer to the first rules on Artificial Intelligence’ (2023) <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence> [Accessed: 2023-05-11].

European Parliament ‘2021/0106(COD) Artificial Intelligence Act’ <https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0106(COD)&l=en> [Accessed: 2023-05-15].

Gutierrez D ‘AI Black Box Horror Stories - When Transparency was needed’ (2019) <https://opendatascience.com/ai-black-box-horror-stories-when-transparency-was-needed/> [Accessed: 2023-05-08].

Kiener M, ‘‘You may be hacked’ and other things doctors should tell you’ (2020 <https://theconversation.com/you-may-be-hacked-and-other-things-doctors-should-tell-you-148946> [Accessed: 2023-05-15].

Mueller B ‘How Much Will the Artificial Intelligence Act Cost Europe?’ (2021) <https://datainnovation.org/2021/07/how-much-will-the-artificial-intelligence-act-cost-europe/> [Accessed: 2023-05-07].

Mueller B ‘The Artificial Intelligence Act is a Threat to Europe’s Digital Economy and Will Hamstring the EU’s Technology Sector in the Global Marketplace’ (2021) <https://datainnovation.org/2021/04/the-artificial-intelligence-act-is-a-threat-to-europes-digital-economy-and-will-hamstring-the-eus-technology-sector-in-the-global-marketplace/> [Accessed: 2023-05-07].

World Health Organisation (WHO) & Office of the united nations High Commissioner for Human Rights 'The Right to Health, Fact sheet' <https://www.ohchr.org/sites/default/files/Documents/Publications/Factsheet31.pdf> [Accessed: 2023-04-07].

Cases

European Union

Court of Justice of the European Union

CJEU Judgement, 5 February 1963, in case C-26/62. *Van Gend en Loos.* [ECLI:EU:C:1963:1].

CJEU Judgement, 15 July 1964, in case C-6/64. *Costa v. ENEL.* [ECLI:EU:C:1964:66].

CJEU Judgement, 30 January 1974, in case C-148/73. *Raymond and Marie Louwage.* [ECLI:EU:C:1974:7].

CJEU Judgement, 6 November 2003, in case C-101/01. *Lindqvist.* [ECLI:EU:C:2003:596].

CJEU Judgement, 13 May 2014, in case C-131/12. *Google Spain and Google*. [ECLI:EU:C:2014:317].

CJEU Judgement, 6 October 2015, in case C-362/14. *Schrems*. [ECLI:EU:C:2015:650].

CJEU Judgement, 18 June 2015, in case C-508/13. *Estonia*. [ECLI:EU:C:2004:443].

CJEU Judgement, 16 July 2020, in case C-311/18. *Facebook Ireland and Schrems*. [ECLI:EU:C:2020:559].

Tribunal of Justice of the European Union

Judgment of the General Court, 17 March 2016, in case T-817/14. *Zoofachhandel Züpke and others*. [ECLI:EU:T:2016:157].

European Court of Human Rights

Judgment 14.3.2013 [Section I], 14 March 2013, in case note 161. *Bernh Larsen Holding AS and Others.*