FACULTY OF LAW
Lund University

Magdalena Rietzler

Who is responsible if an AI system gives a wrong diagnosis?

Analysis of the EU liability law framework of medical AI

JAEM03 Master Thesis

European Business Law
30 higher education credits

Supervisor: Ana Nordberg
Term: Spring 2022

Abstract

AI systems are part of our daily lives and not only science fiction. In the healthcare sector are medical AI systems used to monitor patients, compare x-rays in order to detect diseases, or to even make a diagnosis. These AI systems help healthcare providers to make the work of doctors and nurses more efficient and to ensure the best service for their patients. However, next to these benefits come such new technologies also with never-before-seen challenges. The media reports, e.g. about cyberattacks or data leaks which can lead to data theft. But what happens when not only the data gets stolen, but the medical AI system gives a wrong diagnose which leads to the wrong treatment? Or who is liable if an AI system discriminates and prefers white over black patients? These questions have led to discussions in the EU and its member states since years and the first guidelines as well as legal frameworks have been presented to tackle the issues of AI. This thesis analysis the current legal framework of the EU as well as the German legislation as an example for national law to see if the current legal liability framework is sufficient to tackle these new issues. Whereas fundamental rights and the GDPR have efficient safeguards in place to tackle liability issues of AI systems, the Product Liability Directive does not cover these systems enough. However, the European Commission is aware of this and has already conducted a public consultation about a revision of this directive. Furthermore, examines this work if the AI Act and the European Parliament's resolution on civil liability for AI can close the gaps. Both proposals follow a risk-based approach, however, the AI Act does not entail liability rules, but it introduces obligations and requirements for high-risk AI systems to make them safe. This framework is a good starting point in order to tackle challenges which arise from the use of AI systems.

Table of Content

Abbreviations

AI	Artificial Intelligence
BGB	Bürgerliches Gesetzbuch (German Civil Code)
BGBl.	Bundesgesetzblatt (German Federal Law Gazette)
BverfG	Bundesverfassungsgericht (German Consitutional Court)
CJEU	Court of Justice of the European Union
COM	Communication
COMPAS	Correctional Offender Management Profiling for Alternative Sanctions
CRi	Computer Law Review International
EDPB	European Data Protection Board
EECC	European Electronic Communications Code
EU	European Union
ECHR	European Convention on Human Rights
ENISA	European Union Agency for Cybersecurity
EUCFR	European Charter of Fundamental Rights
GDPR	General Data Protection Regulation
IIA	Inception impact assessment
INL	Legislative initiative procedure
IoT	Internet of Things
JIPITEC	Journal of Intellectual Property, Information Technology and Electronic Commerce Law
M-EPLI	Maastricht European Private Law Institute
ProdHaftG	Produkthaftungsgesetz (German Product Liability Act)
StGB	Strafgesetzbuch (German Criminal Code)

1 Introduction

1.1 Background

New technologies such as AI are changing our world by shifting how people communicate, work, and live. People use virtual assistants and self-driving cars, search online for partners, or 'google' their symptoms when they are feeling ill instead of seeing a doctor.[1] AI systems bring many opportunities and benefits with them and the European Commission[2] as well as Member states[3] have recognised how important it is to invest in this area.[4] Additionally, AI improves inter alia healthcare by making diagnosis more precise or enabling a better prevention of diseases.[5] For example, in Denmark there is an AI system in place which helps emergency services to save lives by making a diagnosis based on the sound of the caller's voice. Furthermore, radiologists in Austria detect tumours more accurately by comparing x-rays with other data.[6]

Next to these benefits, AI comes with potential risks and challenges. For example, opaque decision-making, sexist and racist discrimination, being used for criminal purposes or intrusion in our private lives.[7] Ursula von der Leyen said in her guidelines for the next European Commission: 'I want Europe to strive for more by grasping the opportunities from the digital age within safe and ethical boundaries'. Further, von der Leyen said: 'We will jointly define standards for this new generation of technologies that will become the global norm'.[8] In 2018 the European Commission presented the 'European strategy for AI' to address the

[1] Arjun Panesar, *Machine Learning and AI for Healthcare; Big Data for improved health outcomes* (apress 2019) XXV.
[2] European Commission, 'Advancing the IoT in Europe' (Commission Staff Working Document) SWD(2016) 110 final; European Commission, 'Building a European Data Economy' (Communication) COM(2017) 9 final; European Commission, 'AI for Europe' (Communication) COM(2018) 237 final; European Commission, 'Coordinated Plan on AI' (Communication) COM(2018) 795 final.
[3] See e.g. French AI Strategy Report >https://www.aiforhumanity.fr/en/< accessed 12 May 2022; German AI Strategy >https://www.ki-strategie-deutschland.de/home.html?file=files/downloads/Nationale_KI-Strategie_engl.pdf< accessed 12 May 2022; Swedish AI Strategy Report >https://www.government.se/4a7451/contentassets/fe2ba005fb49433587574c513a837fac/national-approach-to-artificial-intelligence.pdf< accessed 12 May 2022.
[4] European Commission, 'Report on the safety and liability implications of AI, IoT and robotics' (Communication) COM(2020) 64 final, 1.
[5] European Commission, 'White Paper on AI' (Communication) COM(2020) 65 final, 1.
[6] European Commission, 'AI for Europe' COM(2018) 237 final, 1.
[7] European Commission, 'White Paper on AI' COM(2020) 65 final, 1.
[8] Ursula von der Leyen, 'A Union that strives for more; My agenda for Europe' 13 >https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf< accessed 10 May 2022.

aforementioned challenges and risks of AI. Since then, the European Commission as well as the European Parliament introduced further documents regarding the regulation of AI systems.[9]

The main goal of the European liability framework is to ensure that all products and services function safely, reliably and that occurring damages will be compensated. However, AI and other technologies change the attributes of products and services[10] and therefore it must be investigated if new rules for medical AI are needed or if the current legal framework entails enough safeguards. In 2020, as part of the EU digital strategy, the European Parliament published a resolution[11] about a civil liability regime for AI and the European Commission proposed its AI Act[12] in 2021. This thesis examines these two documents in Chapter 5.

1.2 Purpose and research questions

The main purpose of this thesis is to evaluate if there are sufficient safeguards in the EU liability systems to protect patients from harmful medical AI systems. In doing so this thesis evaluates the current legal liability framework of medical AI in the EU and analyses if the current legislation is sufficient or if there are gaps which must be filled. Furthermore, this work investigates if the proposed AI Act and the European Parliament's 'resolution with recommendations to the Commission on a civil liability regime for AI' could help to close such occurring gaps. Considering the purpose of this thesis, the following research questions will be addressed:

1) *Do gaps exist in the current legal liability framework of EU law with respect to medical AI? If so, where in this framework are the gaps?*

2) *Can the proposed AI Act and the European's Parliament's 'resolution* with recommendations to the Commission on a civil liability regime for AI' *close the possible liability gaps in the medical sector under EU law?*

[9] European Commission, 'AI for Europe' COM(2018) 237 final.
[10] European Commission, 'Report on the safety and liability implications of AI, the IoT and robotics' (Communication) COM(2020) 64 final, 1.
[11] European Parliament`, 'European Parliament resolution of 20 October 2020 with recommendations on the Commission on a civil liability regime for AI' 2020/2014(INL).
[12] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on AI (AI Act) and amending certain Union legislative acts' COM(22.1) 206 final.

1.3 Methodology and Materials

In order to answer the research questions in section 1.2, this thesis uses mainly the doctrinal legal method. This research method aims to 'give a systematic exposition of the principles, rules and concepts governing a particular legal field or institution and analyses the relationship between these principles, rules and concepts with a view to solving unclarities and gaps in the existing law'.[13] This method conducts research in primary law, secondary law, and case law to examine *de lege lata* as well as in legal commentary in order to get an understanding of how the law should be (*de lege ferenda*).[14]

Next to the doctrinal method will section 4.4 apply the German classical interpretation method to analyse the existing German legal liability framework. According to the German Constitutional Court, the classical method is formed by four types of interpretation. These are the interpretation from the wording of the norm (grammatical interpretation), from its context (systematic interpretation), from its purpose (teleological interpretation), and from the legislative materials and the history of its origin (historical interpretation).[15]

Furthermore, additional materials are used to address the research questions in section 1.2. These include primary and secondary sources of EU law, like the treaties, regulations, directives, and the jurisprudence of the Court. Because of the novelty of the topic and the fast-moving environment of AI, research articles, publications as well as blog posts and expert studies are used as well.

1.4 Delimitations

Although there are several types of new technologies with important legal liability questions, such as IoT and robotics, this thesis focuses on AI systems applied to the medical sector. There are challenges and risks that may arise in many sectors that introduce AI systems. However, the associated legal liability questions are especially important in the medical sector as errors may cause enormous harm and even cost lives.

[13] Jan M. Smits, 'What is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research' (2015) 2015/06 M-EPLI Working Paper.
[14] Mike McConville and Wing Hong Chui, 'Research Methods for Law' (2nd Edition, Edinburgh University Press, 2017).
[15] Ivo Bach, 'Einführung in die Juristische Methodenlehre' [2020/2021] >https://www.uni-goettingen.de/de/document/download/83cfd1ca6a8f15427fbd6cc039250e6d.pdf/Methodenlehre%20-%20Skript%202020.pdf< accessed 23 May 2022; BVerfG 17.5.1960, 2 BvL 11/59 and 11/60, BverfGE 11, 126.

This work is a European law thesis and therefore does not cover technical terms. Most AI systems require research level expert knowledge to understand them. Therefore, this thesis provides only a short working definition, which is found in section 2.1.

In chapter 4.1.1, Germany is used as an example of a national liability regime as part of the existing legal liability framework of medical AI. Germany is chosen as an example because of its dominant political position and the influence on other Member states law systems. Furthermore, 'the additional value of German tort law is that it is the most elaborated and systematized tort law system in Europe, and possibly in the world, which makes it an important source for legal questions and answers'.[16]

1.5 Outline

This thesis contains six chapters including the introductory chapter. In order to answer the research questions from section 1.2, the second chapter defines the term 'AI' and shows the challenges which medical AI systems may face. After giving this background information the third chapter introduces the legal liability categories as well as the groups of people who could be held liable if an AI system causes damage or harm. Further, chapter four shows the existing legal framework in the EU in regard to the liability of AI systems. By doing so, this chapter elaborates on current EU legislation and German liability law as an example for national law. Chapter five presents the European Parliament's resolution on civil liability rules regarding AI[17] and the proposed AI Act from the European Commission[18]. Further, chapter five analysis these two documents and discusses if they are sufficient tools to close possible gaps in the current EU liability framework. Lastly, chapter six ends this thesis with a conclusion and a summary about the findings.

[16] Cees van Dam, *European Tort Law* (Oxford, 2013) 10.
[17] European Parliament`, 'European Parliament resolution of 20 October 2020 with recommendations on the Commission on a civil liability regime for AI' 2020/2014(INL).
[18] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on AI (AI Act) and amending certain Union legislative acts' COM(22.1) 206 final.

2 AI in the Medical Sector

Automated as well as AI algorithmic systems help humans to make crucial decisions in a wide range of areas.[19] An example for such an AI system the COMPAS system, which entails an algorithm to conduct a recidivism risk assessment and helped judges in the US to make the decision, if defendants should be detained in custody or should be released while awaiting trial.[20] The medical sector uses AI systems in various ways such as 'diagnosing patients, end-to-end drug discovery and development, improving communication between physician and patient, transcribing medical documents, such as prescriptions, and remotely treating patients.'[21]

2.1 Definition of Artificial Intelligence

There is a collective understanding that 'AI' is intelligence shown by machines with minimal human intervention.[22] The European Commission shares this view by saying that 'AI refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals'.[23] However, different types and subfields of AI exist and AI systems can be purely based on software or AI can be embedded in hardware devices.[24]

2.1.1 Virtual branch

The virtual branch represents Machine Learning, or also called Deep Learning, where mathematical algorithms improve learning through experience. Further, Machine Learning algorithms can be allocated into three categories: (1) unsupervised, (2) supervised, and (3) reinforcement learning. Unsupervised in this context is the ability to find patterns, whereas in supervised Machine Learning the classification and prediction algorithms are based on

[19] Hao-Fei Cheng and others, 'Explaining Decision-Making Algorithms through UI: Strategies to Help Non-Expert Stakeholders' (2019) 559 CHI Paper, 1.
[20] Sam Corbett-Davies and others, 'Algorithmic decision making and the cost of fairness' [2017] >https://arxiv.org/pdf/1701.08230.pdf< accessed 07 March 2022.
[21] Kanadpriya Basu and others, 'AI: How is It Changing Medical Science and Its Future?' (2020) 65(5) Indian Journal of Dermatology, 365.
[22] Jason Chung and Amanda Zink, 'Hey Watson – Can I Sue You for Malpractice? Examining the Liability of AI in Medicine' (2018) 11 2 Asia Pacific Journal of Health Law & Ethics 51, 53.
[23] European Commission, 'AI for Europe' (Communication) COM(2018) 237 final, p. 1.
[24] Ibid, p. 1.

previous examples. Besides that, uses reinforcement learning 'sequences of rewards and punishments to form a strategy for operation in a specific problem space'.[25]

Genetics and molecular medicine already use AI successfully by applying machine learning algorithms and knowledge management to improve discoveries. Another successful example for AI usage in healthcare are unsupervised protein-protein interaction algorithms which have led to new therapeutic targets.[26]

Moreover, electronic medical records are part of the virtual AI branch. In these records are certain algorithms used to identify subjects which have, for example, a family history of hereditary disease or a risk of a chronic disease. In this context AI enables individuals to capture, share and apply their knowledge to help improve organisational knowledge and therefore to make the optimal decision in real time.[27] Besides that, AI tools were developed which can help healthcare providers to filter clinically-relevant insights from free text which is e.g., contained in medical records or insurance claims.[28] One example for such an AI tool is the Healthcare Natural Language API which has been released by Google Cloud in 2018.[29]

2.1.2 Physical branch

The physical branch includes physical objects, medical devices and increasingly sophisticated carebots. The medical sector uses carebots as helpers to provide care services[30]and as assistant surgeons or solo practitioners in the field of surgery.[31] However, before the medical sector uses such robots on a daily basis, the legislators must solve ethical[32] and liability issues. Section 2.2 of this thesis further elaborates on these issues.

[25] Pavel Hamet and Johanne Tremblay, 'AI in medicine' (2017) 69 Metabolism Clinical and Experimental 36, 37.
[26] Ibid; See for more information: Konstantinos Theofilators and others, 'Predicting protein complexes from weighted protein-protein interaction graphs with a novel unsupervised methodology: Evolutionary enhanced Markov clustering' (2015) 63, 3 AI Med.
[27] Pavel Hamet and Johanne Tremblay, 'AI in medicine' (2017) 69 Metabolism Clinical and Experimental 36, 38.
[28] Simone Edelmann, '4 key benefits of applying AI to medical records' (*HealthcareTransformers*, 21 July 2021) >https://healthcaretransformers.com/digital-health/ai-improves-electronic-health-records/< accessed 05 April 2022.
[29] William McKnight and Jake Dolezal, 'Healthcare Natural Language Processing' (*Gigaom*, 16 March 2022) >https://gigaom.com/report/healthcare-natural-language-processing/< accessed 05 April.
[30] Pavel Hamet and Johanne Tremblay, 'AI in medicine' (2017) 69 Metabolism Clinical and Experimental 36, 39.
[31] Jeffrey A. Larson, Michael H. Johnson, and Sam B. Bhayani, 'Application of Surgical Safety Standards to Robotic Surgery: Five Principles of Ethics for Nonmaleficence' (2014) 218(2) Journal of the American College of Surgeons 290.
[32] Pavel Hamet and Johanne Tremblay, 'AI in medicine' (2017) 69 Metabolism Clinical and Experimental 36, 39.

2.2 Challenges of AI in the medical sector

As the examples in section 2.1 show, AI brings great benefits into daily lives and especially the medical sector profits from this technology. Furthermore, medical AI helps to ease and improve the work of medical personnel, and the use of such technology can help to prevent human errors caused by negligence.[33] Nevertheless, next to these benefits occur concerns around the use of medical AI systems. These concerns are, in example, the risk of bias, the black box problem which leads to a lack of clarity of AI algorithms as well as privacy and security issues which arise naturally because of the sensitive data which accumulate in medicine.

2.2.1 Bias of and discrimination through AI

The training of AI models requires a large amount of input or so-called training data.[34] Bias can occur, if such training data is inaccurate or under representative. An example for under representative data is societal discrimination which can occur from poor access to health care for a certain group of people in society. Besides that, can an AI system become biased if the training data consists of a small sample (e.g. minority groups).[35] Having under representative data can perpetuate or exacerbate health disparities.[36]

Biased algorithms in healthcare can lead to underestimation or overestimation of risks in certain patient groups. Humans have biases too because the notion of bias is complex, and it will not be possible to develop a completely unbiased AI system. However, it should be possible, and consequently ethically necessary, to develop such systems which help to balance human biases and therefore to have fairer outcomes.[37] Additionally, the bias reduction through AI is important to achieve improved as well as more equitable health outcomes.[38]

---

[33] Sri Sunarti and others, 'AI in healthcare: opportunities and risk for future' (2021) 35(1) Gaceta Sanitaria 67, 68 f.

[34] Sandeep Reddy and others, 'A governance model for the application of AI in health care' (2020) 27(3) Journal of the American Medical Informatics Association 491, 492.

[35] Ibid, 492.

[36] Julia Angwin and others, 'Machine Bias' (*ProPublica*, 23 May 2016) >https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing< accessed 10 April 2022.

[37] Danton S. Char, Nigam H. Shah, and David Magnus, 'Implementing machine learning in healthcare-addressing ethical challenges' (2018) 378 (11) N Engl J Med 981.

[38] Sandeep Reddy and others, 'A governance model for the application of AI in health care' (2020) 27(3) Journal of the American Medical Informatics Association 491, 492.

Next to bias can lead these flawed datasets to 'misleading predictions, adverse events, and even large-scale discrimination'.[39] 'Discrimination refers to an unjustified distinction of treatment on the basis of any physical or cultural trait, such as gender [and] race'.[40] Discriminatory AI systems can, for example, occur through flawed data collection or aggregation[41], as well as through ethical issues. AI systems learn from their 'fed' data and if these datasets are discriminatory, the AI system learn these patterns and discriminate certain group of people.[42]

2.2.2 Black box problem

The black box problem is another challenge that arises from the use of AI systems in health care. In the field of computing a black box can be a device, a program, or a system where you can see the input and output, but have no insight into the processes and operations in between.[43] Consequently, the black box problem arises because it is often difficult to understand how AI systems operate and how they make their decisions.[44] Or in other words: The AI system does not 'explicitly share how and why it reaches its conclusions'. For a high amount of AI tools, it is not important how the systems generate their outputs, but as soon as the answer is 'unexpected, incorrect, or problematic' it turns into a 'black box problem'.[45]

Especially tools that use artificial neural networks and deep learning suffer from the black box problem. An easy way to describe artificial neural networks is that these networks consist of hidden layers of nodes. Each of these nodes processes the given input and passes the output to the next layer of nodes. The term 'deep learning' describes a large artificial neural network, with a high number of these hidden layers. Further, can this large artificial neural

[39] Sri Sunarti and others, 'AI in healthcare: opportunities and risk for future' (2021) 35(1) Gaceta Sanitaria 67, 68 f.
[40] Andrea Romei and Salvatore Ruggieri, 'Discrimination Data Analysis: A Multi-discriplicary Bibliography' in: Bart Custers and others (eds.) *'Discrimination and Privacy in the Information Society'* (2013) Chapter 6, p. 109.
[41] Alexander Tischbirek, 'Artificial Intelligence and Discrmination: Discriminating Against Discriminatory Systems' (2020), in: Thomas Wischmayer and Timo Rademacher (eds.) '*Regulating Artificial Intelligence'* > (Springer, 2020) p. 104 f.
[42] Further elaboration on iscrimination by AI systems would extend the ambit of this thesis; See for more information on discriminatory AI systems: Magdalena Rietzler, 'Are AI systems sexist and racist? Gender and Race Discrimination by AI' (2021).
[43] Think Automation, 'The AI black box problem' >https://www.thinkautomation.com/bots-and-ai/the-ai-black-box-problem/< accessed 10 April 2022.
[44] Carlos Zednik, 'Solving the Black Box Problem: A Normative Framework for Explainable AI' >https://arxiv.org/ftp/arxiv/papers/1903/1903.04361.pdf< accessed 10 April 2022.
[45] Think Automation, 'The AI black box problem' > https://www.thinkautomation.com/bots-and-ai/the-ai-black-box-problem/< accessed 10 April 2022.

network learn on its own by recognising patterns. Because of this vast number of layers, it is impossible to understand what the nodes have learned and to see the output between layers.[46]

In addition, several reasons exist why algorithmic systems can be black boxes. One of these reasons is the lack of technical expertise to understand the complexity of the used algorithms and how the AI systems make their decisions. However, it is not always a question of expertise because even experts struggle sometimes to understand how the AI systems they build will behave in practice and use the fed data.[47]

Next to these technical issues in relation to the black box problem arise also ethical concerns. AI systems are becoming increasingly part of our daily lives and its decisions have more serious impact. If an AI system is, e.g. used to detect cancer and makes a mistake, this can lead to serious consequences. However, AI systems can make mistakes the same way as humans do, but these systems lack the ability to understand if their output is ethically correct. Therefore, humans have to analyse the outcome of AI applications, and this is not possible, if humans do not understand how the system came to its decision.[48]

2.2.3 Privacy issues

Healthcare data is traditionally considered as a sensitive type of data and therefore needs a special degree of protection, because this type of data 'can go to the very core of a human being'.[49] The respect for a person's privacy is an important ethical principle in the medical sector because privacy is linked to the patient's autonomy or self-determination, personal identity, and well-being. Therefore, it is important to maintain patient confidentiality and ensure adequate procedures to obtain genuine, informed consent from patients for both health care interventions and the use of their personal health information.

Recent examples have shown how easily such a data breach can happen and how sensitive healthcare data has been published without the patient's consent.[50] For example, the Royal Free London NHS Foundation Trust shared patient data in line with the development of

[46] Think Automation, 'The AI black box problem' > https://www.thinkautomation.com/bots-and-ai/the-ai-black-box-problem/< accessed 10 April 2022.
[47] Frederik J. Zuiderveen Borgesius, 'Strengthening legal protection against discrimination by algorithms and AI' (2020) 24 The Internatinal Journal of Human Rights 1572, 1577.
[48] Think Automation, 'The AI black box problem' > https://www.thinkautomation.com/bots-and-ai/the-ai-black-box-problem/< accessed 10 April 2022.
[49] University of Groningen, 'Sensitive data and medical confidentiality' >https://www.futurelearn.com/info/courses/protecting-health-data/0/steps/39608< accessed 23 May 2022.
[50] Sandeep Reddy and others, 'A governance model for the application of AI in health care' (2020) 27(3) Journal of the American Medical Informatics Association 491, 492.

a clinical application without the consent of patients.[51] Another data breach was conducted by Klarna Bank AB, which has been fined by the Swedish Authority for Privacy Protection because the company 'did not provide information on the purpose and the legal basis for which personal data was processed in one of the company's services'.[52] Furthermore, Apoteket, a Swedish state-owned pharmacy chain, shared around a million customer details with Facebook.[53]

Further, there is a growing concern that anonymized data can be re-identified with a few spatiotemporal data points, which can lead to a mistrust of patients. There may also be concerns about the method of data collection for training AI models. As mentioned in section 2.2.2, the training of high-quality AI algorithms require large datasets and therefore, patient data may be collected by healthcare providers without informing patients about the ultimate use of the collected data. For instance, AI tools may collect data while assisting the elderly in their homes without them knowing and without them giving their consent.[54]

2.2.4 Security issues

Healthcare providers increasingly use AI systems to e.g., monitor patients and for their record management.[55] Certainly, these new AI-based solutions increase the productivity of medical staff as well as the clinical benefits of patient-level information, but they also raise the complexity and risk of security issues.[56] These issues can be practical or regulatory. An example for a practical challenge is to ensure that the collected patient data 'can be extracted, decrypted, and analyzed'.[57] A regulatory challenge, on the other hand, is to make sure that the data from patients and healthcare providers are protected by law.

New types of security issues that may arise from AI, and are particularly damaging to sensitive health data, are for example cybersecurity attacks in form of system manipulations,

[51] Julia Powles and Hal Hodson, 'Google DeepMind and healthcare in an age of algorithms' (2017) 7 Health and Technology 351.
[52] EDPB, 'The Swedish Authority for Privacy Protection (IMY) issues an administrative fine against Klarna Bank AB after investigation' (5 April 2022), >https://edpb.europa.eu/news/national-news/2022/swedish-authority-privacy-protection-imy-issues-administrative-fine-against_en< accessed 15 April 2022.
[53] Sveriges Radio, 'Apoteket apologizes for sharing around a million customer details to facebook' >https://sverigesradio.se/artikel/apoteket-apologizes-for-sharing-around-a-million-customer-details-to-facebook< accessed 22 May 2022.
[54] Sandeep Reddy and others, 'A governance model for the application of AI in health care' (2020) 27(3) Journal of the American Medical Informatics Association 491, 492.
[55] Taher M. Ghazal, 'Internet of Things with AI for HealthCare Security' (2021) Arabian Journal for Science and Engineering >https://link.springer.com/content/pdf/10.1007/s13369-021-06083-8.pdf< accessed 20 April 2022.
[56] Jakub P. Hlávka, 'Security, privacy, and information-sharing aspects of healthcare AI' in Adam Bohr and Kaveh Memarzadeh (eds.), '*AI in Healthcare'* (Elsevier Inc. 2020), Chapter 10, p. 235.
[57] Ibid, p. 235.

data poisoning[58], or malicious attacks[59]. Besides that, the incorrect implementation of AI systems can pose another security threat. Data poisoning can occur in two ways: (1) Injecting information into the system to obtain a wrong classification, and (2) Threat actors may use the training data to open a backdoor. One example for the second possibility is that a malware is placed in a system and this malware decides when and where is the best time for an attack.[60] Malicious attacks can be triggered by malware such as viruses, spyware, or worms. For example, if a user clicks on a malicious link or email attachment, the virus installs a malicious software on the device and gives the attackers access to the device.[61]

2.3 Interim result

This section shows how essential the role of AI systems in the medical sector is. However, it also shows that AI systems bring issues with them. These issues include the potential bias in AI systems, the black box problem as well as privacy and security issues. Especially in the medical sector such issues can lead to serious consequences for the individual patient/data subject, for example, not only to the fact that you do not get a job in a hiring process, but to serious physical or mental harm of patients. Therefore, it is important to have a legal framework which prevents such issues but also helps victims to get compensation in case something happens through using AI in medicine.

[58] Sue Poremba, 'Data Poisoning: When Attackers Turn AI and ML Against You' (*Security Intelligence*, 21 April 2021) >https://securityintelligence.com/articles/data-poisoning-ai-and-machine-learning/< accessed 20 April 2022.
[59] Elizabeth Fichtner, 'Cybersecurity 101: Intro to the Top 10 Common Types of Cybersecurity Attacks' (*datto*, 31 January 2022) >https://www.datto.com/blog/cybersecurity-101-intro-to-the-top-10-common-types-of-cybersecurity-attacks< accessed 21 April 2022.
[60] Sue Poremba, 'Data Poisoning: When Attackers Turn AI and ML Against You' (*Security Intelligence*, 21 April 2021) >https://securityintelligence.com/articles/data-poisoning-ai-and-machine-learning/< accessed 20 April 2022.
[61] Elizabeth Fichtner, 'Cybersecurity 101: Intro to the Top 10 Common Types of Cybersecurity Attacks' (*datto*, 31 January 2022) >https://www.datto.com/blog/cybersecurity-101-intro-to-the-top-10-common-types-of-cybersecurity-attacks< accessed 21 April 2022.

3 Liability Law and AI

Chapter two has shown that AI comes not only with a high number of benefits but also with great challenges. Especially in the medical sector can these issues cause serious harm to patients. AI algorithms in healthcare are for example used to select the needed medication, to make accurate diagnosis, to predict patient risks, or to prioritise patients to receive or allocate limited healthcare resources.[62] These issues raise questions such as: Who is liable if an AI system discriminates female patients?, Who is responsible if sensitive patient data gets leaked?, or Who is responsible if AI systems give a wrong diagnosis?.

At this point liability law, as one part of the legal framework of AI, steps in. With the introduction of new technologies liability law can lead to an increase in welfare. Furthermore, from an economic point of view, liability rules can help to internalise risks and thus create incentives for the beneficial use of new technologies such as AI.[63]

3.1 Legal liability categories

According to the Cambridge Dictionary liability is 'the fact that someone is legally responsible for something'.[64] Furthermore, the concept of liability plays a very important role in our lives. Firstly, it gives a person who has suffered harm or damage the right to claim and receive compensation from the person who is liable for the harm or damage, and secondly, it gives needed incentives for natural and legal persons to avoid causing such harm or damage in order to not to have to pay for it.[65]

3.1.1 Fault-based liability

Fault-based liability or also called negligence liability is the standard liability principle in most EU member states.[66] Since it presupposes a duty breach in addition to damage and causality, it serves as an instrument to influence the level of care. Furthermore, fault-based liability can be avoided if the required level of care is observed.

[62] Nicholson W. Price,'AI in health care: applications and legal implications' (2017) 14(1) The SciTech Lawyer 10.
[63] Herbert Zech, 'Liability for AI: public policy considerations' (2021) ERA Forum 147, 150.
[64] Cambridge Dictionary, Definition of 'liability'.
[65] European Parliament`, 'European Parliament resolution of 20 October 2020 with recommendations on the Commission on a civil liability regime for AI' 2020/2014(INL), p 3.
[66] Gerhard Wagner, 'Robot liability' in Sebastian Lohsse, Reiner Schulze, and Dirk Staudenmeyer (eds.), *Liability for AI and IoT* (Nomos, 2019), pp. 27, 33.

The negligence liability only applies if the person who caused the damage did not exercise the due level of care. The judiciary determines the duties of care, and these define the level of care. To determine the duties of care makes the judiciary an assessment based on 'potential social benefits of a conduct' and the risks.[67] However, the judiciary can only conduct this assessment if it has sufficient knowledge about the possible risks in the field of AI.

In addition, negligence liability creates an incentive for potential victims, to ensure that no damages occur. Potential victims (or also called affected persons) are, e.g. users or other third parties. If, for example, the manufacturers and operators have behaved dutifully, they are not liable, and those affected persons are liable for damage themselves.[68] This is also called the 'general risk of living'.[69] Therefore, affected persons have an incentive to do everything in their power to avoid such damage. However, the requirement is that the potential victim is able to avoid the damage because an average person often does not have sufficient knowledge about AI risks. Furthermore, AI applications exist that one cannot escape in everyday life. Consequently, in such cases those affected persons cannot avoid certain risks. Therefore, 'fault-based liability for many new technologies leads to the promotion of technologies at the expense of those affected'.[70]

3.1.2 Strict liability

The AI Act[71] introduces a strict liability scheme for high-risk AI systems. Strict liability affects both the level of care and the level of activity because they fully internalise the economic AI risks and thus activate private risk knowledge. Furthermore, it creates incentives for the development of existing technologies and arguably contributes to public acceptance. In addition, strict liability is used as a risk-sharing tool, particularly when combined with compulsory liability insurance (third party insurance). However, strict liability, like any other liability rule, just works if there is proof of individual causation.

According to the level of activity, strict liability assigns the economic risk to the injurer, regardless of whether they act dutifully or not. Therefore, the risk controller must evaluate if the expected benefit of an activity is higher than its risk and if the risk is higher, the activity should not be conducted. Through delegating the assessment to the developers and users of the

[67] Herbert Zech, 'Liability for AI: public policy considerations' (2021) ERA Forum 147, 151.
[68] Ibid, 151.
[69] Ibid, 151.
[70] Ibid, 151.
[71] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on AN (AI Act) and amending certein Union legislative acts' (Communication) COM(2021) 206 final; See further information about the AI Act in chapter five.

AI technologies, private risk knowledge is made available. Usually, the operators and manufacturers have more risk knowledge as the legislator, executive, or judiciary, therefore it makes sense to delegate the assessment to the operators and manufacturers. Moreover, strict liability has the incentive effect to further develop technologies in order to make them safer and to increase the user's trust. If the technology does not seem safe to users, they will refuse to use it. Besides that, the developers want to provide safe products to decrease the liability risk.

According to critics hinders the strict liability concept innovation. However, strict liability does not prohibit the use of new technologies, but merely requires users of the technology to consider whether they want to use it. It may be that legislation introduces direct prohibitions because otherwise the risks cannot be assessed. Therefore, strict liability is a good regulatory instrument which allows to deal with a situation of uncertain risk assessment. Strict liability should provide legal certainty and clarify existing liability risks because it is 'the liability for actions that are fundamentally desired by society, and for which the appropriate incentives should be provided'.[72]

3.1.3 Product liability

Product liability is harmonised in Directive 85/374/EEC.[73] Although it does not directly require negligence, the producer's negligence is included in the defect requirement of the Directive. Following, product liability 'can be seen as de facto negligence liability'.[74] Consequently, the same public policy rationales apply to product liability as to fault-based liability. Besides that, 'the burden of proof is not shifted completely' and therefore, the injured party must prove the defectiveness of a product.[75]

3.2 Who could be liable?

After analysing the different legal liability categories it is important to introduce the actors. Or in other words: The possible group of people who could be liable for harm or damage of another person through medical AI. In the lifecycle of an AI system are many actors involved, and an explanation of them is needed, because the questions arise how obligations should be

[72] Herbert Zech, 'Liability for AI: public policy considerations' (2021) ERA Forum 147, 152 f.
[73] Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member states concerning liability for defective products 85/374/EEC L 210/29 (Product Liability Directive); See further information on Directive 85/374/EEC in section 4.4.2.
[74] Herbert Zech, 'Liability for AI: public policy considerations' (2021) ERA Forum 147, 154.
[75] Ibid, 154.

distributed. According to the European Commission should in a future legal framework 'each obligation be addressed to the actor(s) who is (are) best placed to address any potential risk'.[76] For example, developers are responsible to control the risk during the development phase.[77] However, it is important to mention that the different stakeholders have different levels of knowledge about innovative technologies such as AI and thus also about the risks associated with it. Liability law must take these different levels of knowledge into account in its assessment.[78] The literature uses different names for these actors, but this thesis follows the terms which are used in the AI Act.[79]

Firstly, Art. 3(2) of the AI Act defines provider as 'a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge'. Next to providers are according to Art. 3(3) AI Act small-scale providers which are providers who are a micro or small enterprise within the meaning of Commission Recommendation 2003/361/EC. The Commission's Recommendation sets the limits for staff headcount and financial ceilings which count as recognition criteria for micro and small enterprises.[80]

Secondly, Art. 3(4) AI Act defines users as any natural or legal persons, public authorities, agencies, or other bodies using an AI system under its authority, except where the AI system is used during a personal non-professional activity. Therefore, can users be professional or private users.[81]

Furthermore, an authorised representative is per Art. 3(5) AI Act 'any natural or legal person established in the Union who has received a written mandate from a provider of an AI system to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation'. Therefore, a provider who has not established itself in the EU can make its AI system in the EU through an authorised representative available. To do so, the provider can give the authorised representative all necessary information about the compliance of the AI system, which it wants to bring on the EU market. This must be done through a written mandate and can be important if an importer cannot be identified.[82]

---

[76] European Commission, 'White Paper on AI' COM(2020) 65 final, 22.
[77] Ibid, 22.
[78] Herbert Zech, 'Liability for AI: public policy considerations' (2021) ERA Forum 147, 150
[79] See further elaborations about the AI Act in context of the topic of this thesis in chapter 5.
[80] European Commission, 'Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises' 2003/361/EC L 124/36.
[81] European Commission, 'White Paper on AI' COM(2020) 65 final, 22.
[82] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on AN (AI Act) and amending certein Union legislative acts' COM(2021) 206 final, recital 56.

Art. 3(6) AI Act defines the term ‘importer’ as ‘any natural or legal person established in the Union that places on the market or puts into service an AI system that bears the name or trademark of a natural or legal person established outside the Union’.

Moreover, distributor ‘means any natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market without affecting its properties’ (Art. 3(7) AI Act).

To conclude the actors, according to Art. 3(8) AI Act can an operator be ‘the provider, the user, the authorised representative, the importer and the distributor’.

3.3 Interim result

The third chapter shows how complex liability rules are and how many different actors play a role in relation to the liability of AI systems. Because not every actor can be held equally liable, these actors must be identified and determined in liability questions. Furthermore, the respective level of knowledge of the actors must be considered, because a private user cannot have the same level of knowledge about an AI system as the producer and therefore different liability rules should apply to these groups. The following chapters will show how the legislators of the EU and the member states try to solve the liability issues in accordance with the AI system in the medical sector.

4 Existing legal framework for medical AI

The main goal of the EU legal liability framework is to make sure that all products and services which are placed on the market are safe, reliable, and consistent. In addition, the compensation for damages should be ensured. Especially for products and services that incorporate new technologies, high safety standards as well as a mechanism to ensure remedies for damages, help to strengthen consumer protection. Furthermore, the EU legal liability framework contributes to increasing trust in new technologies and their adoption by industry and users. Besides the strengthening of consumer protection creates a liability scheme certainty for businesses.

Currently, the EU has a harmonised regulatory framework in place to ensure product liability which combined with national, non-harmonised liability rules, helps to tackle liability issues. However, new technologies such as AI, IoT[83], and robotics also raise new liability issues, because they change the attributes of products and services which may be not covered by the current legal liability framework.[84]

An important note is that the primarily responsibility for health protection lies with the Member states. However, the Union has the competence to adapt legislation which improves public health, prevents, and manages diseases, and mitigates sources of danger to human health.[85]

4.1 Fundamental Rights

The European Commission states in its 'White Paper on AI' from February 2020 that AI has a substantial influence on our society and that 'it is vital that European AI is grounded in our values and fundamental rights such as human dignity and privacy protection'.[86] Fundamental rights are as a part of primary EU law clear guidelines for medical AI. Therefore, fundamental rights give a basic framework for the development and application of AI in the medical sector.[87]

[83] ENISA defines IoT as 'a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making'.
[84] European Commission, 'Report on the safety and liability implications of AI, the IoT and robotics' COM(2020) 64 final, 1.
[85] European Parliament, 'Public Health' (Factsheet) > https://www.europarl.europa.eu/ftu/pdf/en/FTU_2.2.4.pdf< accessed 5 May 2022.
[86] European Commission, 'White Paper on AI' COM(2020) 65 final, 2.
[87] David Schneeberger, Karl Stöger, and Andreas Holzinger, 'The European Legal Framework for Medical AI' [2020] IFIP 209 f.

Furthermore, the EU legislator must respect fundamental rights when drafting and adopting secondary legislation such as regulations and directives concerning liability in the medical AI.

The EU Charter is the main source of the fundamental rights framework in the EU and is strongly influenced by the ECHR, which is also applicable in all EU Member states. The provision of medical services is protected by the freedom to provide services and therefore the EU Charter is fully applicable to medical AI. Medical AI is especially a relevant field in relation to fundamental rights, because a malfunction can cause big harm to a person's physical and mental health and therefore could have profound consequences.

Fundamental rights have two main purposes: (1) The protection of individuals from state intervention, and (2) The obligation of the state 'to protect certain freedoms from interference by third parties'.[88] In order to fulfil its 'obligation to protect', the state can, for example, enact appropriate laws governing relations between private individuals or create special approval procedures for the placing on the market of goods or services that could jeopardise the fundamental rights of their users. For that reason, the 'obligation to protect' is very important in medicine.[89] According to the European Court of Human Rights, the state is obliged under fundamental rights to regulate the provision of health services in such a way that precautions are taken against serious damage to health caused by inadequate services.[90] Based on this, the state has to make sure that, e.g. healthcare providers implement quality assurance measures as well as that they respect the necessary 'level of care'.

In summary, developers, and providers of AI tools for healthcare as well as the EU Member states must conform with fundamental rights because it is a binding legal framework. The human oversight criteria, the right to protection of life and private life, anti-discrimination, and the protection of personal data are especially important fundamental rights in relation to AI in the medical sector.[91]

4.2 Product Safety Law

As in section 4.1 mentioned, the EU legislator must in the drafting and adopting of secondary legislation guarantee the compliance with fundamental rights. One part of the secondary law

[88] David Schneeberger, Karl Stöger, and Andreas Holzinger, 'The European Legal Framework for Medical AI' [2020] IFIP 209 f.
[89] Ibid, 209 f.
[90] David Harris and others, *Law of the European Convention on Human Rights*, (4th edn, Oxford University Press 2018).
[91] David Schneeberger, Karl Stöger, and Andreas Holzinger, 'The European Legal Framework for Medical AI' [2020] IFIP 210.

framework of medical AI and especially liability law is Product Safety Law. According to product safety law, an assessment of a medical AI product's safety standards is needed before it can be placed on the EU market. The goal of product safety law is 'to minimise the risk of harm by a faulty product'.[92] The product safety law in the EU consists of the two Medical Devices Regulations[93] as well as the Product Liability Directive.

4.2.1 Medical Devices Regulations

On 26 May 2021 new rules on medical devices entered into application. These new rules include the Regulation 2017/745 on medical devices and the Regulation 2017/746 on in vitro diagnostic medical devices. These two regulations are intended to establish a 'more robust regulatory framework to protect public health and patient safety'.[94]

Despite the novelty of these two regulations, they do not directly regulate AI products or list these types of products as a specific category. Nevertheless, AI applications can be usually allocated to software, which the manufacturer intended to use for specific medical purposes in the treatment of human beings. Therefore, AI applications, which are used for the treatment of patients or for other medical purposes, will be classified as medical devices and fall most probably under the ambit of one of the two regulations.

If a medical AI application falls into a certain risk classification[95], it can be possible that a conformity assessment procedure[96] has to be conducted. Part of this assessment are, for example, certifications, reviews as well as clinical evidence. Unfortunately, machine learning systems often do not fall into the ambit of the risk classification of the Medical Devices Regulations, because the software definition and its allocated risk are inflexible. Further the definition does not distinguish between static and machine learning systems and therefore miss to mention risks which are special to machine learning. Such risks can be for example the black box problem, its dynamic nature, and the problem that false positive or false negative outcomes can occur.[97] However, the European Commission is aware of the special risks of machine

[92] David Schneeberger, Karl Stöger, and Andreas Holzinger, 'The European Legal Framework for Medical AI' [2020] IFIP 210.
[93] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices [2017] OJ L 117/1 (Medical Devices Regulation); Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices [2017] OJ L 117/176 (In-Vitro Diagnostic Devices Regulation).
[94] European Commission, 'Public health: Stronger rules on medical devices' (Press realease, 26 May 2021) >https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2617< accessed 19 May 2022.
[95] Medical Devices Regulation, Art. 51.
[96] Medical Devices Regulation, Art. 52.
[97] David Schneeberger, Karl Stöger, and Andreas Holzinger, 'The European Legal Framework for Medical AI' [2020] IFIP 216.

learning and mentions in its White Paper on AI that a sufficient legal framework in this regard is needed.[98]

Medical devices, which are in conformity with the regulation 2017/745, get a CE marking granted by a notified body, which shows that a medical device is approved to enter the EU market. Further, this applies to medical AI applications which are used as a therapeutic or diagnostic tool, because they bear a medium (or also called potential) risk and therefore require approval to access the market.[99] The CE marking shows that the products meet the high safety standards as well as health and environmental protection requirements.[100] Explainability is not part of these requirements, however, transparency should be important in this regard to prove that the system 'does not mistake mere correlations within data for causality'.[101] Furthermore, explainability could be helpful for risk management as well as to avoid liability for, e.g. doctors who use medical AI.[102]

4.2.2 Product Liability Directive 85/374/EEC

Liability law in the EU consists of non-harmonised national civil liability law and harmonised product liability law.[103] Part of the harmonised framework is Directive 85/374/EEC on liability for defective products (Product Liability Directive). The Product Liability Directive came into force in 1985 and sets out the EU-wide applicable liability regime for defective products. The main reason for the adoption of this directive was to ensure that manufacturers take responsibility towards customers for defective products.

Furthermore, this directive introduces strict liability rules for producers, which means that the producers are responsible for defective products, even if they are not responsible for the fault. Another goal of the directive is to contribute to economic growth by creating a stable

[98] European Commission, 'White Paper on AI - A European approach to excellence and trust', COM(2020) 65 final, p. 12.
[99] Medical Devices Regulation, Art. 20; David Schneeberger, Karl Stöger, and Andreas Holzinger, 'The European Legal Framework for Medical AI' [2020] IFIP 217; Phg foundation, 'Algorithms as medical devices' (2019) >https://www.phgfoundation.org/media/74/download/algorithms-as-medical-devices.pdf< accessed 25 April 2022.
[100] European Commission, Single market and standards, 'CE marking' >https://ec.europa.eu/growth/single-market/ce-marking_de< accessed 25 April 2022.
[101] David Schneeberger, Karl Stöger, and Andreas Holzinger, 'The European Legal Framework for Medical AI' [2020] IFIP 217.
[102] David Schneeberger, Karl Stöger, and Andreas Holzinger, 'The European Legal Framework for Medical AI' [2020] IFIP 217; Philipp Hacker and others, 'Explainable AI under contract and tort law: legal incentives and technical challenges' (2020) 28 415 >https://link.springer.com/content/pdf/10.1007/s10506-020-09260-6.pdf< accessed 25 April 2022.
[103] David Schneeberger, Karl Stöger, and Andreas Holzinger, 'The European Legal Framework for Medical AI' [2020] IFIP 218.

and legal environment for equal competition that enables companies to bring innovative products to the market.[104] However, the Directive does not harmonise product liability matters which are outside its scope. Therefore, the member states can provide their own product liability law by other causes of action. However, the national laws have to be consistent with the Product Liability Directive.[105]

Since 1985 products, technologies as well as the economy have evolved drastically and therefore also the challenges and risks for the stakeholders. However, the EU reacted to these changes and has evolved its rules on product safety since the directive came into force. In 2018 the European Commission assessed the Product Liability Directive. Part of this assessment was to evaluate if the directive 'remains relevant by embracing recent technological changes' and if it is a sufficient tool to tackle cybersecurity challenges as well as autonomous devices.[106] The European Commission concluded that the Product Liability Directive is still an adequate tool but also noted that some clarifications regarding emerging new technologies are needed.[107]

Next to the concerns about new technologies, the European Commission discussed in its report the issues of liability rules in regard to healthcare products. Between 2011 and 2017 the CJEU ruled on four judgments concerning medical devices and pharmaceutical products. These judgements show the specific problems with this product category.[108] One judgment concerned a case where a hospital bed burned a patient during surgery and the Court confirmed the fact that the Product Liability Directive applies just to producers, and not to service providers who may use defective products.[109] Nevertheless, member states can still introduce national legislation which establishes strict liability rules for service providers as long as these national laws are coherent with the directive and do not restrict the producers strict liability.[110]

---

[104] European Commission, 'Report on the application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member states concerning liability for defective products (85/374/EEC)' COM(2018) 246 final.

[105] Rod Freeman and others, 'Product liability and safety in the EU: overview' (2022) > https://uk.practicallaw.thomsonreuters.com/w-013-0379?transitionType=Default&contextData=(sc.Default)&firstPage=true< accessed 17 May 2022; Case C-310/13 *Novo Nordisk Pharma GmbH v S.* [2014] ECLI:EU:C:2014:2385.

[106] European Commission, 'Report on the application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member states concerning liability for defective products (85/374/EEC)' COM(2018) 246 final, p. 1 f.

[107] European Commission, 'Report on the application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member states concerning liability for defective products (85/374/EEC)' COM(2018) 246 final, p. 1 f.

[108] Ibid, p. 4.

[109] Case C-495/10 *Centre hospitalier universitaire de Besançon v Thomas Dutrueux and Caisse primaire d'assurance maladie du JuraJudgment* [2011] ECLI:EU:C:2011:869.

[110] European Commission, 'Report on the application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member states concerning liability for defective products (85/374/EEC)' COM(2018) 246 final, p. 4 f.

In its report on the safety and liability implications of AI, IoT, and robotics[111] the European Commission discusses further problems regarding new technologies and current liability rules. Especially the burden of proof on the injured person, or in other words, that the victim has to show the causality between the defect product and the damage, raises concerns regarding AI.[112] In detail, civil liability, which can be based on a contract or on tort, is often fault-based and the fault of the liable person, the damage and the causality between the fault and the damage has to be proven.[113] In specific situations like, e.g. the use of dangerous objects, exists next to fault-based liability also strict liability. In this case is the liability for a risk attributed to a specific person and the proof of fault as well as the causality between fault and damage are not important. In most cases these two liability schemes overlap and function together.[114] Furthermore, machine learning algorithms are complex and opaque and therefore it is controversial that the victim has the burden of proof because it will be especially complicated to find a causal link and to trace it back to human behaviour.[115] The discussions in this regard go from that the medical service provider should bear the burden of proof[116] to the demand of a strict liability scheme for AI tools.[117] Chapter six of this thesis entails further details about the current developments in the evolution of the Product Safety Directive and the future of EU Product Safety Law.

4.3 Data Protection Law

EU Data Protection Law is an important part of the EU liability framework regarding medical AI, because it sets standards for regulating data processing that both protect the rights of

[111] European Commission, 'Report on the safety and liability implications of AI, the IoT and robotics' COM(2020) 64 final.
[112] Ibid; David Schneeberger, Karl Stöger, and Andreas Holzinger, 'The European Legal Framework for Medical AI' [2020] IFIP 218.
[113] European Commission, 'Report on the safety and liability implications of AI, the IoT and robotics' COM(2020) 64 final.
[114] David Schneeberger, Karl Stöger, and Andreas Holzinger, 'The European Legal Framework for Medical AI' [2020] IFIP 218.
[115] European Commission, 'Report on the safety and liability implications of AI, the IoT and robotics' COM(2020) 64 final.
[116] Daniel Schönberger, 'Artificial intelligence in healthcare: a critical analysis of the legal and ethical implications' (2019) 27 International Journal of Law and Information Technology, 171.
[117] Gerald Spindler, 'Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz - Braucht das Recht neue Haftungskategorien?' (2015) 31 Computer und Recht, 766; Herbert Zech, 'Künstliche Intelligenz und Haftungsfragen' (2019) 5 Zeitschrift für die gesamte Privatrechtswissenschaft 5, 198.

individuals and impose obligations on data controllers[118] and processors[119].[120] Furthermore, the personal data[121] which is stored and processed[122] in healthcare is especially sensitive and data breaches or cyberattacks can be extremely harmful for patients. Therefore, the GDPR puts safeguards in place to prevent such data breaches or cyberattacks so that no damage occurs, and liability law has to intervene.

The key principle of the GDPR, which came into force on 25 May 2018, is the transparency requirement in Art. 5(1) a. Linked to this are lawfulness and fairness, which are both part of accountability (Art. 5(2) GDPR). These principles are important in discussion about the GDPR.[123]

The GDPR introduced changes about the responsibility and liability of controllers and processors in the liability scheme of EU Data Protection Law. In the GDPR as well as in Directive 95/46/EC[124], which was the main source of Data Protection Law before the GDPR repealed it, the controller is still primarily responsible for compliance. According to Art. 82(2) GDPR, processors are liable if they act non-compliant towards data subjects. Certainly, there exist also cases where two or more providers or controllers are involved, in these situations every controller or processor can be liable if the damage results from its failure to comply with its obligations by the GDPR (cumulative liability scheme).[125]

[118] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of the personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR)' (2016) OJ L 119/1, Art. 4(7) defines 'controller' as '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'.

[119] Art. 4(8) GDPR defines 'processor' as 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'.

[120] WHO Guidance, 'Ethics and Governance of AI for health' (2021), >https://apps.who.int/iris/rest/bitstreams/1352854/retrieve< p. 19.

[121] Art. 4(1) GDPR defines 'personal data' as 'information relating to an identified or identifiable natural person (data subject); an identifiable natural person is who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

[122] Art. 4(2) GDPR defines 'processing' as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organi sation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.

[123] David Schneeberger, Karl Stöger, and Andreas Holzinger, 'The European Legal Framework for Medical AI' [2020] IFIP 212.

[124] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L 281/31.

[125] Brendan Van Alsenoy, 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation', 7 (2016) JIPITEC 271, para 38.

4.3.1 Prohibition of decisions based only on automated processing

Art. 22 GDPR aims to prevent the determination of individuals as mere objects if a process is conducted solely by a machine and therefore is constituted as an automated decision-making.[126] This is especially important in healthcare because such a situation would lead to the loss of autonomy as well as human control and responsibility.[127] Furthermore, Art. 22 GDPR makes sure that the final decision in an automated decision-making process is made by a human and prohibits decisions made solely by machines. This prohibition does not affect systems, where a human being has any time the possibility to intervene and to change the decision. An example for such a decision-support systems is an AI system which gives recommendations for a diagnosis to a doctor. However, in case a nurse uses the same system, and she is advised to follow the AI system's recommendations without questioning them, the system is classified as fully automated decision-making and therefore prohibited.

In general, a decision based on a fully autonomous approach is only prohibited if it has serious consequences. However, because of the special circumstances in healthcare, medical AI systems without a human in the loop are always prohibited.[128] To this full prohibition exist exceptions. Art. 22(4) GDPR entails the most important exception - the explicit written or electronic consent of the patient where they agree with the fully automated processing of their health data. The second exception, which should be interpreted narrowly, is that the processing of medical data can be necessary because of substantial public interest (public health). One example could be the importance of finding vulnerable groups who are most affected by the COVID-19 pandemic to protect them. However, it must be noted that this exception cannot be used as a blanket exception to easily circumvent the prohibition.[129]

[126] David Schneeberger, Karl Stöger, and Andreas Holzinger, 'The European Legal Framework for Medical AI' [2020] IFIP 212.
[127] Lee A. Bygrave, 'Minding the machine v2.0; The EU general data protection regulation and automated decision-making' in Karen Yeung and Martin Lodge (eds) *Algorithmic Regulation*, (Oxford University Press, 2019) pp. 248–262 >https://doi.org/10.1093/oso/9780198838494.001.0001< accessed 03 May 2022.
[128] David Schneeberger, Karl Stöger, and Andreas Holzinger, 'The European Legal Framework for Medical AI' [2020] IFIP 212; Art. 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (2018) WP251rev.01.
[129] David Schneeberger, Karl Stöger, and Andreas Holzinger, 'The European Legal Framework for Medical AI' [2020] IFIP 212; European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679' (2020) Version 1.1 >https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf< accessed 02 May 2022.

4.3.2 Controller liability

According to Art. 82(2) GDPR can controllers, if they engage in processing, be 'liable for the damage caused by processing which infringes this Regulation'. Therefore, controllers are mainly liable for any damages which arise from unlawful data processing. Art. 82(3) GDPR gives an exemption of this strict liability 'if it proves that it is not in any way responsible for the event giving rise to the damage'. Note that the exemption of Art. 82(3) GDPR only applies to events which are beyond the control of the controller. These are, for example, extraordinary circumstances which cannot be avoided with any reasonable measures, and which is not the risk materialisation for which the person is strictly liable.[130]

4.3.3 Processor liability

The GDPR imposes obligations on processors in case they act non-compliant towards data subjects (Art. 82(2)). Furthermore, the GDPR entails in Art. 28(3) a provision which binds the processors legally to the controllers. Therefore, processors must comply with directly applicable requirements and with requirements imposed by way of contract.[131] As mentioned in section 4.3.2, controllers can principally be liable for any kind of infringement which can occur in accordance with the GDPR. Processors, on the other hand, can be liable according to Art. 82(2) GDPR for non-compliance with their obligations which arise from the GDPR (e.g., Art. 30(2), Art. 33(2), Art. 37, Arts. 41 and 42 GDPR) or if they act outside or contrary to lawful instructions of the controller. In theory, processors are liable in relation for its part in the processing. This is sometimes in the literature called 'proportional liability'.[132]

However, the processor can be liable for the entire damage if they are responsible for the suffered harm (Art. 82(4) GDPR). More precisely, processors can be liable if they act contrary to or outside of the controller's instructions and only if the processor is clearly responsible for the damage, they can be liable for the entire damage. Nevertheless, note that there exist no thresholds regarding the 'degree of responsibility of the processor in contributing to the damage.'[133] Consequently, the processor could be held liable for the whole damage, even if they were just partially responsible.[134]

[130] Brendan Van Alsenoy, 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation', 7 (2016) JIPITEC 271, para 44.
[131] Ibid, para 50.
[132] Ibid, paras 51 and 52.
[133] Brendan Van Alsenoy, 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation', 7 (2016) JIPITEC 271, para 53.
[134] Ibid, para 53.

In conclusion, the controller is mainly responsible for the processing and can therefore be held liable if an unlawful processing activity happens, but in addition has the data subject the option to sue the processor if there is a reason that the processor could be responsible for the damage. Therefore, the data subject can choose who they want to sue for the damage (the controller or the processor).[135]

4.4 National Laws

As the previous elaborations of chapter four show, the harmonised part of EU Liability Law consists of EU legislation in form of directives and case law of the CJEU and the ECHR. This section gives an insight into the second part of EU Liability Law of the non-harmonised rules which exist in the EU member states. However, because of the open borders some national laws have influenced other member states laws. For example, the French liability law has influenced the tort law of Belgium, Italy, the Netherlands, Poland, and Spain, whereas German liability law has left its traces in Austrian, Bulgarian, Czech, Greek, Latvian, Portuguese, Slovakian, and Slovenian law.[136] This section will show as an example of a national non-harmonised legislation the German liability law and discusses, if the current legal liability framework in Germany is sufficient to tackle liability issues of medical AI.

4.4.1 German Liability Law

The German liability system is based on misconduct that leads to damage. However, not everyone who engages in misconduct is legally punishable. According to German law, only those who have legal personality by law can be liable. This is not yet the case with robots and machines, which is why the misconduct of a human being behind the AI must be considered.[137] Following, German law sets out different liability rules for the different actors. Actors can be producers, operators, and users.

[135] Ibid, para 54; If the controller and processor are part of the same judicial proceeding, the compensation may be divided proportionate to the responsibility of the damage and if they part of different judicial proceedings, the controller can claim back the compensation from the processor they had to pay for damages responsible by the processor (Art. 82(5) GDPR).
[136] Cees van Dam, *European Tort Law* (Oxford, 2013) 9.
[137] Simone Rosenthal and Philipp Müller-Peltzer, 'Künstliche Intelligenz - wer haftet, wenn ein Roboter versagt?' (2019) >https://www.srd-rechtsanwaelte.de/blog/kuenstliche-intelligenz-haftung/< accessed 05 May 2022.

4.4.1.1 ProdHaftG - German Product Liability Law

The ProdHaftG sets out the product liability rules in Germany. The ProdHaftG is the transposition of the Product Liability Directive 85/374/EEC into the German legislation and came into force on 15 December 1989, over one year later as it was supposed to be implemented. § 1(1) ProdHaftG lays out the requirements for the liability of a producer: (1) Violation of a protected legal interest (e.g. killing of a person, injury to body or health, damage to an object), (2) through a defective product, (3) with a financial damage, which result from this defective product (causality), and (4) as well as no existence of a legal exception (§1(2), (3) ProdHaftG).

From these four prerequisites, it can be concluded that the producers are in most cases liable for violations of protected legal interests caused by an AI system which was developed by the producer. Furthermore, the liability of producers is a strict liability and therefore, it is irrelevant whether the injured party is at fault for the violation of the legal interest. The only decisive factor for liability is that the producer has created a source of danger by putting this defective product on the market and the violation of the legal interest and the damage of the product can be attributed to him.

However, because of the black problem it can be difficult to prove programming errors. Therefore, the injured party has to prove the error and the liability of the producers often fail because of this precondition.[138]

4.4.1.2 Producer liability

Next to the possible liability of the producer under the ProdHaftG, there is also producer liability. The producer's liability results from the claim for damages under §823(1) BGB. This claim for damages is not only applicable to producers, instead it applies to everyone who violates one of the in §823(1) BGB mentioned legal properties. However, producer liability has special conditions under this provision. In contrast to product liability, which is part of strict liability, the producer must have been responsible for placing a defective product on the market, i.e., negligently, or intentionally.

Normally, the injured party would have to prove that the producer intentionally put a defective product on the market. The burden of proof is reversed in product liability under §823(1) BGB: The producer must exonerate himself, i.e. prove that he did not put a defective

[138] Simone Rosenthal and Philipp Müller-Peltzer, 'Künstliche Intelligenz - wer haftet, wenn ein Roboter versagt?' (2019) >https://www.srd-rechtsanwaelte.de/blog/kuenstliche-intelligenz-haftung/< accessed 05 May 2022.

product on the market. The reason for this reversal of the burden of proof is that the injured person rarely has insight into the production process or the code of the AI system, and after the ProdHaftG does not apply in these cases, the victim can rely on §823(1) BGB.[139]

4.4.1.3 Operator and User liability

Operators and users may also be liable under § 823(1) BGB, but in this case without the special requirement that applies to producers. Instead, the user is liable if the operation of the AI has negligently or intentionally caused an injury to a legal interest, which are according to § 823(1) BGB life, body health, property, or other rights, which has led to a damage.

The problem which can arise here, will often be the 'fault' requirement. For example, how can a patient (user) judge whether the doctor who uses an AI system for his or her diagnosis has complied with the required due diligence. Additionally, the doctor (operator) most probably does not understand on what the medical AI system based its decision and therefore he or she is not able to say what constitutes the failure of the system. Following, it can be assumed that in the case where the operator has operated the AI system correctly, the operator is not responsible for any errors. In particular, the rules of producer liability do not apply here. The injured party would therefore have to prove that the AI operator did not observe the due care required during business. In practice, this usually turns out to be difficult.[140]

4.4.1.4 Medical Liability and Patient Rights Law

Next to the Liability rules in German law is the so-called *Arzthaftungsrecht* (Medical Liability Law) a part of the German legal framework in the medical sector.

According to § 1(2) of the (Model-) Professional Code for Doctors Practising[141] in Germany it is the task of doctors 'to preserve life, to protect and restore health, to alleviate suffering, to assist the dying and to participate in the preservation of the natural foundations of life in view of their importance of human health'.[142] Therefore, patients who seek medical care can expect treatment that is in line with current medical knowledge and the standard of

[139] Simone Rosenthal and Philipp Müller-Peltzer, 'Künstliche Intelligenz - wer haftet, wenn ein Roboter versagt?' (2019) >https://www.srd-rechtsanwaelte.de/blog/kuenstliche-intelligenz-haftung/< accessed 05 May 2022.
[140] Ibid.
[141] The (Model-) Professional Code of Conduct contains the professional and ethical foundations of the medical profession. It serves the medical associations as a model for their professional regulations and thus contributes to a development of professional law that is as uniform as possible throughout Germany.
[142] Bundesärztekammer, '(Muster)-Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte, MBO-Ä 1997 in der Fassung des Beschlusses des 124. Deutschen Ärztetages vom 05. Mai 2021 in Berlin' (Bekanntmachung) >https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Recht/_Bek_BAEK_MBO-AE_Online_final.pdf< accessed 05 May 2022.

medicine. If the doctor does not comply with these requirements, he or she is liable for any resulting damage to health. This Medical Liability is regulated in §§ 630 a f. BGB as a contract liability, § 280(1) BGB as compensation of damages for breach of duty, and in § 823 f. BGB as an unlawful action, because every curative intervention also constitutes intentional or at least negligent bodily harm, which only remains unpunished if the patient has effectively consented within the meaning of § 228 StGB. Medical Liability comes into play when the doctor violates his or her obligations under the treatment contract with the patient and a treatment error happens. Note that the contract between the doctor and the patient is a service contract and therefore, the doctor only owes the patient a careful and professional treatment but no healing success or a successful treatment.[143]

Next to this exists in Germany a Patient Rights Law, which came into force on the 26 February 2013, and helps to strengthen the role of the patients as well as putting them on an equal level as the doctor. Part of this framework is the embedding of the treatment contract in the German Civil Code. Further, patients must be informed comprehensively about the treatment, such as the diagnosis and the right therapy. Another patient right is that there is more transparency and openness for liability cases due to treatment and information errors. The law stipulates that, under certain conditions, the treating person is obliged to admit his or her own errors and to disclose the errors of other treating persons.[144]

Regarding Patient Rights and the use of medical AI, Germany took the first steps to tackle the issues of new technologies by introducing the Digital Healthcare Act in November 2019. The main goal of the Digital Healthcare Act is to improve the healthcare provision in Germany through digitalisation and innovation. Following novelties are included in the Digital Healthcare Act: Patients will be able to use healthcare apps more easily and quickly, an electronic patient record system will be introduced, the possibility of online video consultations will be made available, as well as electronic prescriptions will be possible. Unfortunately, there are no liability rules for AI in healthcare included in this Act, but it is a good start that obligations to improve IT security in practices of non-hospitals doctors and dentists will be introduced to put more safeguards for sensitive patient data in place.[145]

---

[143] Deutscher Bundestag, 'Grundzüge der Arzthaftung in Deutschland aus zivil- und strafrechtlicher Perspektive' (2021) WD 7 - 3000 - 091/21.

[144] Patientenrechtegesetz, BGBl. I 2013, 277; Bundesministerium der Justiz, 'Patientenrechte' (2021) >https://www.bmj.de/DE/Themen/VorsorgeUndPatientenrechte/Patientenrechte/Patientenrechte_node.html< accessed 06 May 2022.

[145] Federal Ministry of Health, 'Driving the digital transformation of Germany's healthcare system for the good of patients' (2020) >https://www.bundesgesundheitsministerium.de/en/digital-healthcare-act.html< accessed 10 May 2022; Deutscher Bundestag, 'Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation' (2019) Drucksache 19/13438.

4.4 Soft Law

Besides the harmonised and non-harmonised legal instruments in regard to liability of medical AI exist also soft law in form of guidelines and safety standards[146] which can help to protect patients from harmful use or application of AI systems in their medical treatment. Besides that, the European Commission formed an Expert Group on liability and new technologies, which also contributed to the discussions about AI liability in the EU.[147] Furthermore exist 'Principles of EU Tort Law' which have been collected by the European Group on Tort Law.[148] These principles are a compilation of the basic rules which, despite all the differences in detail, are common to the liability systems of the European states and form the basis of the respective national non-contractual liability law.[149]

4.5 Interim Result

In its White Paper on AI states the European Commission that 'while a number of the requirements are already reflected in existing legal or regulatory regimes, those regarding transparency, traceability and human oversight are not specifically covered under current legislation in many economic sectors.'[150] '[..] [T]his conclusion does not fully hold true for medical AI'. [151] Medical AI is closely linked to questions of fundamental rights, data protection, and autonomy and the current legal framework gives many answers to questions regarding the application of AI. Fundamental rights as well as the GDPR both formulate clear duties to the use of medical AI. For example, informed consent and the requirement to have a 'human in the loop' are essential elements of human oversight. Every AI system which is developed and operated in the EU must be in line with the fundamental rights requirements. Furthermore, the

[146] WHO Guidance, 'Ethics and governance of AI for health' (2021) >https://www.who.int/publications/i/item/9789240029200< accessed 11 May 2022; Council of Europe, 'European ethical Charter on the use of AI in judicial systems and their environment', adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3-4 December 2018).
[147] European Commission, Report of the Expert Group on Liability and New Technologies: 'Liability for AI and other emerging digital technologies' (2019); European Commission, Register of Commission Expert Groups and Other Similar Entities, 'Expert Group on liability and new technologies (E03592)' >https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3592&NewSearch=1&NewSearch=1a< accessed 11 May 2022.
[148] European Group on Tort Law, 'Principles of European Tort Law' >http://www.egtl.org/docs/PETL.pdf< accessed 11 May 2022.
[149] Ulrich Magnus, 'Principles of European Tort Law' (2009) HWB-EuP.
[150] European Commission, 'White Paper on AI' COM(2020) 65 final, 9.
[151] Ibid, 9.

patient has a right to get detailed information about the medical AI which is applied in the treatment process and can make use of the privacy rights stated in the GDPR (e.g., Art. 22(3) GDPR).[152]

According to the current EU Product Liability Law, the product approval procedure and liability in general does not address the use of AI enough. However, the European Commission is already aware of this problem and has started the first steps to solve it by announcing that they will clarify these issues with new market approval procedures for AI systems and a strict liability as well as 'an obligatory insurance scheme for malfunctions of AI'.[153]

[152] David Schneeberger, Karl Stöger, and Andreas Holzinger, 'The European Legal Framework for Medical AI' [2020] IFIP 221.
[153] Ibid, 222.

5 Potential future EU Liability Legal Framework

After analysing the existing legal liability framework in the EU regarding AI systems in the medical sector as well as the issues of such systems and the gaps of the legal framework, it is important to look at the proposed legal framework of the EU, meaning ongoing legislative efforts that combined create a prospective EU legal framework. As mentioned above, there is a debate in the EU, as well as in the member states, concerning the regulation of emerging innovative technologies and on how to tackle new arising challenges, including liability. Part of this discussions are included in AI strategies of several EU Member states[154] and on EU level[155]. In line with the AI strategy on EU level has the European Commission introduced a Proposal for an AI Act and the European Parliament the Resolution 2020/2014 (INL), which both try to give a sufficient harmonised legal framework for alle EU Member states regarding AI. Certainly, the resolution is part of EU soft law, offering an indication of debated policy options and possible legislative direction. Thus, it is crucial to take a closer look, as it plays an essential role in the further development of a legal liability scheme of AI in the Union.

5.1 European Parliament Resolution 2020/2014 (INL)

This section looks more closely at the European Parliament Resolution with recommendations to the Commission on a civil liability regime for AI (2020/2014 (INL)), which have been adopted on 20 October 2020. This resolution entails recommendations for liability rules regarding high-risk AI systems.[156] Moreover, the resolution points out how important a clear and harmonised civil liability scheme in the EU is in order to develop AI technologies as well as to provide legal certainty for users, producers, operators, and other affected persons.[157]

---

[154] See e.g. French AI Strategy Report >https://www.aiforhumanity.fr/en/< accessed 12 May 2022; German AI Strategy >https://www.ki-strategie-deutschland.de/home.html?file=files/downloads/Nationale_KI-Strategie_engl.pdf< accessed 12 May 2022; Swedish AI Strategy Report >https://www.government.se/4a7451/contentassets/fe2ba005fb49433587574c513a837fac/national-approach-to-artificial-intelligence.pdf< accessed 12 May 2022.

[155] European Commission, 'AI for Europe' COM(2018) 237 final

[156] European Parliament, 'European Parliament resolution of 20 October 2020 with recommendations on the Commission on a civil liability regime for AI' 2020/2014(INL).

[157] Henrique Sousa Antunes, 'Civil liability applicable to AI: a preliminary critique of the European Parliament Resolution of 2020' (2020) >https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3743242< https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3743242%3c accessed 12 May 2022.

5.1.1 Background and Objectives

The AI Act[158] is the first possible hard law which has been introduced by the EU to tackle the issues of AI. Before the presentation of the AI Act, the Union has preferred soft law in this regard because it is more flexible and has proven to be compatible with the fast-moving environment of AI systems.[159]

Already in 2017 published the European Parliament a report with recommendations to the EU Commission on the civil law rules on robotics.[160] In this report the European Parliament advised the Commission to formulate a directive on civil law rules on robotics.[161] Followed by that, the Commission appointed in June 2018 the High-Level Expert Group on AI, who published the 'Ethics Guidelines for Trustworthy AI' in March 2019. The aim of the guidelines is to ensure that AI systems are lawful, ethical and robust.[162] Followed by that, in February 2020 the European Commission incorporated these guidelines into its 'White Paper on AI'.[163] In October 2020 the European Parliament released three resolutions with the aim to define the foundation for the future regulation of AI in the EU. These resolutions include the areas ethics[164], intellectual property rights[165], and civil liability[166].

The European Parliament's resolution on the civil liability regime also served as a starting point for the drafting of the AI Act which is aimed to define the obligations of providers and others involved in the production, distribution, and use of AI.[167]

[158] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on AI (AI Act) and amending certain Union legislative acts' COM(2021) 206 final.
[159] Marianna Riedo and Luca Tormen, 'The proposed EU Regulation on AI: A proportional risk-based approach to a civil liability regime for AI' (2021) >https://portolano.it/en/newsletter/litigation-arbitration/the-proposed-eu-regulation-on-ai-a-proportional-risk-based-approach-to-a-civil-liability-regime-for-artificial-intelligence#_ftn2< accessed 18 May 2022.
[160] European Parliament, 'Report with recommendations to the Commission on Civil Law Rules on Robotics' (2017) 2015/2012(INL).
[161] Ibid, recital 65.
[162] European Commission, 'Ethics guidelines for trustworthy AI' (2019) >https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai< accessed 18 May 2022.
[163] European Commission, 'White Paper on AI' COM(2020) 65 final.
[164] European Parliament, 'Resolution on a framework of ethical aspects of artificial intelligence, robotics and related technologies' (2020) 2020/2012(INL).
[165] European Parliament, 'Resolution on intellectual property rights for the development of artificial intelligence technologies' (2020) 2020/2015(INI).
[166] European Parliament, 'European Parliament resolution of 20 October 2020 with recommendations on the Commission on a civil liability regime for AI' 2020/2014(INL).
[167] Marianna Riedo and Luca Tormen, 'The proposed EU Regulation on AI: A proportional risk-based approach to a civil liability regime for AI' (2021) >https://portolano.it/en/newsletter/litigation-arbitration/the-proposed-eu-regulation-on-ai-a-proportional-risk-based-approach-to-a-civil-liability-regime-for-artificial-intelligence#_ftn2< accessed 18 May 2022.

5.1.2 Important provisions

According to Art. 1 of the European Parliament's resolution, the 'Regulation sets out rules for the civil liability claims of natural and legal persons against operators of AI systems.' [168] The Resolution is applicable for both 'frontend operator' and 'backend operator' and applies to cases which are not covered by the Product Liability Directive (Art. 3(d)). Art. 3(e) defines a 'frontend operator' as 'any natural or legal person who exercises a degree of control over a risk connected with the operation and functioning of the AI-system and benefits from its operations'. Art. 3(f), on the other hand, defines a 'backend operator' as 'any natural or legal person who, on a continuous basis, defines the features of the technology and provides data and an essential backend support service and therefore also exercises a degree of control over the risk connected with the operation and functioning of the AI-system'. The European Parliament decided to base the liability rules in their Proposal on operators because they have a certain degree of control over the risks which are connected with the operation and the functioning of an AI system. This is comparable to the owner of a car. The impact to define and influence the algorithm gets higher as more sophisticated and autonomous the system is. Usually, the frontend operator decides how the AI system is used, whereas the backend operator has mostly a higher degree of control over the operational risks.[169] If there exists more than one operator, they are jointly liable (Art. 11).

Additionally, the Proposal follows a risked based approach and applies different liability rules of different risks. Art. 4 of the Proposal introduces a strict liability for high-risk AI systems. 'High risk' in this context 'means a significant potential in an autonomously operating AI-system to cause harm or damage to one or more persons in a manner that is random and goes beyond what can reasonably be expected' (Art. 3(c)). Moreover, Art. 8 lays out a fault-based liability for AI systems, which are not classified as high-risk.

5.2 European Commission Proposal for an AI Act COM(2021) 206 final

In her political guidelines for her tenure leading the European Commission 2019-2024 'A Union that strives for more' states EU Commission's president Ursula von der Leyen that '[…] [d]ata and AI are the ingredients for innovation that can help us to find solutions to societal

[168] European Parliament, 'European Parliament resolution of 20 October 2020 with recommendations on the Commission on a civil liability regime for AI' 2020/2014(INL).
[169] Ibid, recital 10.

challenges, from health to farming, from security to manufacturing'. Further, von der Leyen said that she 'will put forward legislation for a coordinated European approach on the human and ethical implications of AI'.[170] Followed by that, the European Commission published in February 2020 its 'White Paper on AI', which 'sets out policy options on how to achieve the twin objective of promoting the uptake of AI and of addressing the risks associated with certain uses of such technology'.[171] Thereafter, on 21 April 2021, presented the European Commission the Proposal for a Regulation concerning AI.[172] This section talks about the background and the objectives of the AI Act and introduces the important provisions of the Proposal in regard to liability.

5.2.1 Background and Objectives

The European Commission's White Paper discusses policy options to achieve two objectives: (1) The promotion of increasing AI, and (2) to address the risks associated with the use of AI.[173] The proposed AI Act's goal is to implement the second objective by introducing a legal framework to increase trust of EU citizens into AI. Furthermore, the AI Act is 'based on EU values and fundamental rights and aims to give people and other users the confidence to embrace AI-based solutions, while encouraging businesses to develop them'.[174] Besides that, the legal framework regarding AI aims to help increase people's trust in AI systems by making sure that these new technologies are compliant with the law and safe to use.

Another reason for the Proposal was a stakeholder consultation by the European Commission, in which most participants responded that they would support a legal framework to address the challenges and concerns of AI systems. In addition, the European Parliament and the European Council requested legislative action to ensure the well-functioning of the internal market of AI for AI systems at EU level.[175]

[170] Ursula von der Leyen, 'A Union that strives for more; My agenda for Europe' >https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf< accessed 14 May 2022.
[171] European Commission, 'White Paper on AI' COM(2020) 65 final.
[172] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on AI (AI Act) and amending certain Union legislative acts' COM(2021) 206 final.
[173] European Commission, 'White Paper on AI' COM(2020) 65 final.
[174] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on AI (AI Act) and amending certain Union legislative acts' COM(2021) 206 final, p 1.
[175] Ibid, p 1.

Therefore, the AI Act is as the 'first-ever legal framework of AI'[176], the response of the European Commission to the previous discussions and demands of stakeholders and other EU institutions, to tackle the issues arising with AI by providing a legal framework. Further, it was designed to 'guarantee the safety and fundamental rights of people and businesses, while strengthening AI uptake, investment and innovation across the EU'.[177]

5.2.2 Important Provisions

Unfortunately, AI can be misused to manipulate, exploit, and control people. Because of the possible harmful use of AI should certain practices be prohibited if they are in contradiction with the Union's values for human dignity, freedom, equality, democracy, and the rule of law as well as fundamental rights.[178] Therefore, the AI Act is using a risk-based approach to ensure a high level of protection for the values of the EU and the fundamental rights. In line with the introduction of this product safety regime imposes the AI Act market entry requirements and a CE-marking procedure for high-risk AI systems. This section presents the important provisions of the AI Act regarding liability and how it can help to avoid the need to apply liability rules in the first place by preventing harm and damage before they occur.

5.2.2.1 Prohibited AI practices

The Proposal differentiates AI systems based on their possible occurring risks: (1) unacceptable risk, (2) high risk, and (3) low or minimal risk. Art. 5 of the AI Act prohibits certain AI practices which have an unacceptable risk, because they do not fulfil the values of the Union by, e.g. violating fundamental rights.[179] Art. 5(1) prohibits manipulation and exploitation of vulnerabilities which results in physical or psychological harm, social scoring by public authorities, and biometric systems, whereas this provision bans manipulative/exploitative AI systems as well as social scoring in its entirety and real-time and remote biometric identification systems except for certain law enforcement purposes in publicly accessible areas (Art. 5(1) d i-iii).[180]

[176] European Commission, 'Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in AI' (Press release, 21 April 2021) > https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682< accessed 14 May 2022.
[177] Ibid.
[178] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on AI (AI Act) and amending certain Union legislative acts' COM(2021) 206 final, recital 15.
[179] Ibid, explanatory memorandum.
[180] Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU AI Act' (2021) 4 CRi 97, 98; European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on AI (AI Act) and amending certain Union legislative acts' COM(2021) 206 final, recital 15;

Art. 5(1) a and b entails the two prohibited AI practices to regulate manipulation, whereas manipulation in this regard can be understood as that 'the manipulator wants to intentionally but covertly make use of another's decision-making to further their own ends through exploiting some vulnerability'.[181] The Commission has presented in their briefings on the prohibitions examples for both Art. 5(1) a and b, whereas the first could be 'an inaudible sound [...] played in truck drivers' cabins to push them to drive longer than healthy and safe' and the second could be 'a doll with an integrated voice assistant [which] encourages a minor to engage in progressively dangerous behaviour or challenges in the guise of a fun or cool game.'[182]

Next to manipulation, social scoring by public authorities is prohibited. Art. 5(1) c of the AI Act states that 'the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics' is prohibited. Trustworthiness in this context 'can be understood as a combination of attributes that indicate that an entity will not betray another due to bad faith such as misaligned incentives, lack of care, commitment or through competence'.[183]

5.2.2.2 High-risk AI systems

The Proposal sets out classification for high-risk AI systems (Art. 6) and formulates requirements for such qualified high-risk AI systems (Art. 8 - 15) as well as obligations (Art. 16 - 29). Art. 6 AI Act divides high-risk AI systems into two categories: (1) 'AI systems which are intended to be used as a safety component of a product or is itself a product' and therefore already have to go through a third-party assessment process under sectoral legislation, or (2) AI systems, which are not part of another product and used in special areas. These areas mentioned in Art. 7 in combination with Annex III of the AI Act.

DG CONNECT, Gabriele Mazzini, 'A European Strategy for AI' (2nd ELLIS Workshop in Human-Centric Machine Learning (YouTube recording), 10 May 2021) >https://youtu.be/OZtuVKWqhl0?t=10346< accessed 18 May 2022, at 2:52:26 et seq.

[181] Marijn Sax, 'Between Empowerment and Manipulation: The Ethics and Regulation of For-Profit Health Apps' (PhD Thesis, Universiteit van Amsterdam (UvA) 2021) 110–12.

[182] DG CONNECT, Gabriele Mazzini, 'A European Strategy for AI' (2nd ELLIS Workshop in Human-Centric Machine Learning (YouTube recording), 10 May 2021) https://youtu.be/OZtuVKWqhl0?t=10346 accessed 18 May 2022, at 2:52:26 et seq.

[183] Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU AI Act' (2021) 4 CRi 97, 100.

The first category includes AI systems which are safety components in medical devices and therefore, these medical AI systems will be regulated by their sector-specific legislation (see Annex II), the two Medical Devices Regulations. These regulations must be amended to be in line with the obligations of the AI Act. The second category, which talks about AI systems which are not embedded in other products, are qualified as high risks if they are used in specific areas such as e.g., law enforcement or the administration of justice and democratic processes.[184] The healthcare sector is not part of the listed areas in Annex III of the AI Act.

To mitigate the risks of products of the two categories the AI Act puts a CE-marking procedure into place. As mentioned in section 4.2.1, the CE-marking can already be found on many products in the EU, and it shows that a product meets the needed safety, health, and environmental protection requirements. Besides that, a product, which is according to the AI Act classified as high risk, cannot enter the EU market without this CE mark. To get the CE-marking the products have to comply with five requirements: (1) Data and data governance (Art. 10), (2) transparency for users (Art. 13), (3) human oversight (Art. 14), (4) accuracy, robustness, and cybersecurity (Art. 14), and (5) traceability and auditability (Art. 12).[185]

5.2.3 The AI Act and civil liability

The previously presented resolution of the European Parliament on a civil liability regime for AI served as a starting point for drafting the AI Act. Through imposing obligations on providers, distributors, importers, users, and third parties in Art. 16 - 29 follows the AI Act, the approach of the European Parliament.

The European Parliament clarifies 'that AI-systems have neither legal personality nor human conscience'.[186] Further states the European Parliament that the 'opacity and autonomy [of AI systems] could make it very difficult to trace back specific actions to specific human decisions in their design or in their operation. [...] As a result, there might be liability cases in which the allocation of liability could be unfair or inefficient, or in which a person who suffers harm or damage caused by an AI-system cannot prove the fault of the producer, of an

[184] Eve Gaumond, 'AI Act: What is the European approach to AI?' (*Lawfare*, 4 June 2021) > https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai< accessed 18 May 2022.
[185] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on AI (AI Act) and amending certain Union legislative acts' COM(2021) 206 final, Arts. 19, 48 and 49; Eve Gaumond, 'AI: What is the European approach to AI?' (*Lawfare*, 4 June 2021) >https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai< accessed 18 May 2022.
[186] European Parliament, 'European Parliament resolution of 20 October 2020 with recommendations on the Commission on a civil liability regime for AI' 2020/2014(INL), recital 6.

interfering third party or of the operator and ends up without compensation'.[187] However, according to the European Parliament 'it should be clear that whoever creates, maintains, controls or interferes with the AI-system, should be accountable for the harm or damage that the activity, device or process causes.'[188] In recital 53 of the AI Act clarifies the European Commission that 'it is appropriate that a specific natural or legal person, defined as the provider, takes the responsibility for the placing on the market or putting into service of a high-risk AI systems, regardless of whether that natural or legal person is the person who designed or developed the system'.[189] As a consequence, providers must establish 'appropriate data governance and management practices'[190] and fulfil their obligations in order to make sure that risks of AI systems are limited and cause no harm or damage to users or other people.

5.2.4 The AI Act and medical AI

One of the objectives of the AI Act is to turn the EU into the global hub for trustworthy AI and this intention is welcomed by the medical sector. According to experts, the current state of the AI Act in practice may have a disproportionate impact on medical AI, because at its current state are duplications and discrepancies between the two Medical Devices Regulations and the proposed AI Act. To ensure a coherent and clear regulatory environment for manufacturers in the Union, this should be avoided. As mentioned in this thesis have both the Medical Devices Regulations as well as the AI Act certification processes in place and at its current state would the two processes be duplicates. These duplicative certification processes can lead to 'delays in prevention, diagnosis, and care of citizens with life-threatening conditions.'[191] Additionally, can such long processes 'deprive health systems of efficient and high-quality technology.'[192]

5.3 Future developments of Liability Law

Through the Proposal of the European Parliament for a new liability scheme for AI systems and the proposed AI Act as well as the discussions about this topic started the European Commission on the 30 June 2021 an IIA about the revision of safety legislation (e.g., General

[187] European Parliament, 'European Parliament resolution of 20 October 2020 with recommendations on the Commission on a civil liability regime for AI' 2020/2014(INL), recital 7.
[188] Ibid, recital 8.
[189] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on AI (AI Act) and amending certain Union legislative acts' COM(2021) 206 final, rectial 53.
[190] Ibid, recital 44.
[191] Michael Strübin, 'AI in medical technologies: improving the lives of citizens and patients' (2021) 543 The Parliament; Politics, Policy and People Magazine, 12.
[192] Ibid, 12.

Product Safety Directive[193]). The IIA was triggered by an evaluation of the Product Liability Directive in 2018.[194] The aim of this initiative is to rethink the current product liability rules to adapt them to new technologies such as AI to ensure legal certainty and trust for consumers and producers.[195] As part of this IIA conducted the European Commission a public consultation about the civil liability rules in the EU according to AI from October 2021 until January 2022. The goal of this consultation was to collect information from stakeholders about challenges of AI and the views of how to improve the Product Liability Directive. In this public consultation 75% of all respondents[196] expressed their clear support of a need for action to harmonise liability rules on AI in the EU. Further agreed a majority of the respondents that consumers should get compensation for defective products if they caused physical harm or property damages. Besides that, the respondents pointed out that AI systems make it difficult to meet the burden of proof and therefore it is hard to link the damage to a human actor in a highly autonomous AI system.[197] The European Commission's to this initiative is planned for the third quarter of 2022.[198]

5.4 Analysis of the Europeans Parliament's Resolution 2020/2014 (INL) and the proposed AI Act

After analysing the European Parliament's resolution and the proposed AI Act, this section compares the two documents and shows the similarities as well as the differences between them. Furthermore, the relationship between the two documents and liability will be analysed in this section.

[193] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (2001) OJ L 11/4.
[194] European Commission, 'Report from the Commision to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member states concerning liability for defective products (85/374/EEC)' (Communication) COM(2018) 246 final; Rupert Bellinghausen and Kathrin Bauwens, 'Product Liability and AI (Part 2) - The EU Commission's plans for adapting liability rules to the digital age' (*Linklaters*, 16 July 2021) >https://www.linklaters.com/en/insights/blogs/productliabilitylinks/2021/july/product-liability-and-ai-part-2-eu-commissions-plans-for-adapting-rules-to-the-digital-age< accessed 19 May 2022.
[195] European Commission, 'Civil liability - adapting liability rules to the digital age and AI' >https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en< accessed 19 May 2022.
[196] The consultation received a total of 291 responses, whereas 168 answered as organisations and 123 as individuals.
[197] European Commission, 'Civil liability - adapting liability rules to the digital age and AI' >https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en< accessed 19 May 2022.
[198] Ibid.

Both documents follow a risk-based approach, and the AI Act is influenced by the European Parliament's resolution. Whereas the resolution in Art. 4 proposes a strict liability for high-risk AI systems, the AI Act formulates classifications for high-risk AI systems (Art. 6) and sets out requirements (Art. 8-15) and obligations for providers, users, and other parties (Art. 16-29) for such high-risk systems.

The European Parliament does not propose a 'legal revolution' with its resolution and states that the current EU liability framework does not has to be changed completely. Therefore, the Product Liability Directive will still be relevant in the future and can be used to civil liability claims against producers of defective AI systems. The product in this case is the AI system. Nevertheless, a revision of the Directive is needed to include AI systems better. According to the European Parliament some concepts of the Directive should be clarified (e.g. damage, producer, product) and it should be considered to reverse the 'burden of proof' rules for damage caused by digital technologies.[199] Furthermore, the European Parliament says 'that the existing fault-based tort law of the Member states offers in most cases a sufficient level of protection for persons that suffer harm caused by an interfering third party like a hacker or for persons whose property is damaged by such a third party, as the interference regularly constitutes a fault-based action'.[200] However, an addition of liability rules when claims are directed against operators of an AI system seems in view of the European Parliament necessary because the 'operator's liability is justified by the fact that he or she is controlling a risk associated with the AI-system'. It should cover both front-end and back-end operators.[201] The AI Act uses the term 'operator' in another way than the resolution. These different terms and definitions of the actors in the liability scheme can lead to misunderstandings and should be aligned.

The AI Act as well as the resolution and the current movement in the European Commission to adapt the Product Liability Directive are good starting points to tackle the liability issues of new technologies, but until then it is important for parties to define possible liability rules in contracts.[202] Besides that help the imposed requirements on stakeholders as well as the obligations for high-risk systems to prevent harm and damage before it occurs in

[199] Edouard Cruysmans, Cyril Fischer, and Erik Valgaeren, 'Law and AI (part 1): towards a European civil liability regime?' (*Stibbe*, 21 October 2021) >https://www.stibbe.com/en/news/2021/october/law-and-artificial-intelligence-part-one-towards-a-european-civil-liability-regime-the-european-par< accessed 19 May 2022.
[200] European Parliament, 'European Parliament resolution of 20 October 2020 with recommendations on the Commission on a civil liability regime for AI' 2020/2014(INL), Introduction Nr. 9.
[201] Ibid, Introduction Nr. 10 – 12.
[202] Pieter De Grauwe, 'AI & Liability - Whodunit?' (*Gevers*, 13 February 2022) >https://www.gevers.eu/blog/patents/artificial-intelligence-and-liability-whodunit/< accessed 19 May 2022.

order to prevent that liability rules have to step in but of course a sufficient liability framework in regard to AI is needed if something happens.

6 Conclusion

Section 2.2 of this thesis shows issues which may arise with the use of AI systems in the medical sector. For example, AI systems can discriminate people based on their race or gender, sensitive health-data can be leaked through a cyberattack and used for criminal purposes, or an AI system can give a wrong diagnosis to a patient. Naturally, the question arises 'Who can be held liable in such scenarios and is there a sufficient liability framework in place in the EU?'.

Chapter four elaborates on the current legal framework applicable to the liability of AI systems in the EU. This liability framework consists of Fundamental Rights, Product Safety Law, Data Protection Law, German Liability Law as an example for National Law, and Soft Law. Fundamental Rights as well as the GDPR formulate already clear duties to the use of medical AI.[203] Furthermore, Germany has adopted a law regarding autonomous driving which includes liability rules for manufacturers and vehicle owner[204] and the country introduced a Digital Healthcare Act in order to increase patient rights in Germany.[205] However, Germany states that the autonomous driving law is intended to be used temporary until harmonised rules come into force on EU level.[206] Besides that, gaps exist in the current legal framework. Especially the Product Liability Directive does not address the use of AI systems enough, but the EU Commission has already started a consultation to investigate in the possible revision of this Directive.[207] The aim of this consultation is to find out if the Product Liability Directive and 'other national liability rules still provide legal certainty and consumer protection in an age of smart and AI-based products and services.'[208] Experts welcome the European Commission's plans to investigate the change of the Directive and are sure that most issues arising from AI systems could be solved with such a revision.[209]

---

[203] David Schneeberger, Karl Stöger, and Andreas Holzinger, 'The European Legal Framework for Medical AI' [2020] IFIP 221.

[204] Bundesministerium für Digitales und Verkehr, 'Gesetz zum autonomen Fahren tritt in Kraft' (27 July 2021) > https://www.bmvi.de/SharedDocs/DE/Artikel/DG/gesetz-zum-autonomen-fahren.html< accessed 24 May 2022.

[205] Federal Ministry of Health, 'Driving the digital transformation of Germany's healthcare system for the good of patients' (2020) >https://www.bundesgesundheitsministerium.de/en/digital-healthcare-act.html< accessed 10 May 2022.

[206] Bundesministerium für Digitales und Verkehr, 'Gesetz zum autonomen Fahren tritt in Kraft' (27 July 2021) > https://www.bmvi.de/SharedDocs/DE/Artikel/DG/gesetz-zum-autonomen-fahren.html< accessed 24 May 2022.

[207] European Commission, 'Civil liability - adapting liability rules to the digital age and AI' >https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en< accessed 24 May 2022.

[208] European Commission, 'Commission collects views on making liability rules fit for the digital age, AI and circular economy' (20 October 2021) > https://ec.europa.eu/growth/news/commission-collects-views-making-liability-rules-fit-digital-age-artificial-intelligence-and-2021-10-20_en< accessed 24 May 2022.

[209] BEUC, 'Adapting civil liability rules tot he new digital technologies' (6 January 2022) > https://www.beuc.eu/publications/beuc-x-2022-002_response_to_public_consultation_on_pld_and_civil_liability_for_ai.pdf< accessed 24 May 2022.

Besides that, the European Commission proposed the AI Act in April 2021. This Proposal does not include direct liability rules, but it entails obligations and requirements for high-risk AI systems to make them safe. This framework is a good starting point in order to tackle challenges which arise from the use of AI systems.

However, the European Commission has already in its 'Coordinated Plan on AI' from 2021 announced that rules regarding the liability of AI systems will follow in the course of 2022.[210] The expert group for AI, which was appointed by the European Commission, gave already some guidance in regard to possible liability rules: (1) Even when a producer changes a product, which leads to a defect, the manufacturers should be held liable for damages which are caused by their defect product; (2) Operators should be held liable for high-risk AI systems, if they cause damage as result from the operation; (3) It should be kept in mind in regard to defining the primarily operator of a AI product, that servicer provider have a higher degree of control as the AI system's owner/user.[211] Furthermore, the European Commission sees no need to give AI system legal personality.[212]

In conclusion, the EU legislator as well as the Member states are aware of the fact, that the current legal liability framework is not completely sufficient to tackle issues arising from the use of AI. Especially, high-risk areas such as the medical sector need special rules to ensure a safe environment for their patients as well as a legal certainty for healthcare providers. It therefore remains to be seen whether the EU will manage to introduce new legislation in the near future, because technology never sleeps.

[210] Pieter De Grauwe, 'AI & Liability - Whodunit?' (*Gevers*, 13 February 2022) >https://www.gevers.eu/blog/patents/artificial-intelligence-and-liability-whodunit/< accessed 19 May 2022.
[211] Ibid.
[212] European Commission, Report of the Expert Group on Liability and New Technologies: 'Liability for AI and other emerging digital technologies' (2019).

Bibliography

Books

Bygrave L, ‘Minding the machine v2.0. The EU general data protection regulation and automated decision-making’ in Yeung K and Lodge M (eds.), *Algorithmic Regulation* (Oxford University Press, 2019) 248–262

Cormen T H, Leiserson C E, Riveste R L, and Stein C, *Introduction to Algorithms* (3rd edn, The MIT Press 2009)

Harris D, O’Boyle M, Bates E, and Buckley C, *Law of the European Convention on Human Rights* (4th edn, Oxford University Press 2018)

Hlávka J P, ‘Security, privacy, and information-sharing aspects of healthcare AI’ in Bohr A, and Memarzadeh K (eds), *AI in Healthcare* (Chapter 10, Elsevier Inc. 2020) 235-270

Panesar A, *Machine Learning and AI for Healthcare; Big Data for improved health outcomes* (XXV, apress 2019)

Romei A and Ruggieri S, ’Discrimination Data Analysis: A Multi-discriplicary Bibliography’ in: Bart Custers and others (eds.) *’Discrimination and Privacy in the Information Society’* (Chapter 6, Springer 2013)

Tischbirek A, ’Artificial Intelligence and Discrmination: Discriminating Against Discriminatory Systems’ (2020), in: Thomas Wischmayer and Timo Rademacher (eds.) ‘*Regulating Artificial Intelligence’* (Springer, 2020)

Turing A M, *Computing Machinery and Intelligence* (Vol. LIX. No. 236, Mind 1950) 433-460

van Damp C, *European Tort Law* (Oxford, 2013)

Wagner G, ‘Robot liability’ in Lohsse S, Schulze R, and Staudenmeyer D (eds), *Liability for AI and IoT* (Nomos, 2019)

Articles

Antunes H S, 'Civil liability applicable to AI: a preliminary critique of the European Parliament Resolution of 2020' (2020) >https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3743242< https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3743242%3c accessed 12 May 2022

Basu K, Sinha R, Ong A, and Basu T, 'Artificial Intelligence; How is It Changing Medical Science and Its Future?' (2020) 65(5) Indian Journal of Dermatology 365

Char D, Shah N, Magnus D, 'Implementing machine learning in healthcare-addressing ethical challenges' (2018) 378(11) N Engl J Med 2018 981, 983

Cheng H-F, Wang E, Zhang Z, O'Connell F, Gray T, Harper F M, and Zhu H, 'Explaining Decision-Making Algorithms through UI: Strategies to Help Non-Expert Stakeholders' (CHI Paper, 2019) 559

Chung J and Zink A, 'Hey Watson – Can I Sue You for Malpractice? Examining the Liability of Artificial Intelligence in Medicine' (2018) 11(2) Asia Pacific Journal of Health Law & Ethics 51, 53

Corbett-Davies S, Pierson E, Feller A, Goel S, and Huq A, 'Algorithmic decision making and the cost of fairness' (2017) >https://arxiv.org/pdf/1701.08230.pdf< accessed 07 March 2022

De Grauwe P, 'AI & Liability - Whodunit?' (*Gevers*, 13 February 2022) >https://www.gevers.eu/blog/patents/artificial-intelligence-and-liability-whodunit/< accessed 19 May 2022

Edouard Cruysmans, Cyril Fischer, and Erik Valgaeren, 'Law and AI (part 1): towards a European civil liability regime?' (*Stibbe*, 21 October 2021) >https://www.stibbe.com/en/news/2021/october/law-and-artificial-intelligence-part-one-towards-a-european-civil-liability-regime-the-european-par< accessed 19 May 2022

Ghazal T, 'Internet of Things with AI for HealthCare Security' (2021) Arabian Journal for Science and Engineering

Hacker P, Kestrel R, Grundmann S, and Naumann F, 'Explainable AI under contract and tort law: legal incentives and technical challenges' (2020) >https://link.springer.com/content/pdf/10.1007/s10506-020-09260-6.pdf< accessed 25 April 2022

Hamet P and Tremblay J, 'AI in medicine' (2017) 69 Metabolism Clinical and Experimental 36, 37

Larson J, Johnson M, and Bhayani S, 'Application of Surgical Safety Standards to Robotic Surgery: Five Principles of Ethics for Nonmaleficence' (2014) 218(2) Journal of the American College of Surgeons 290

McCarthy J, Minsky M, Rochester N, and Shannon C, 'A proposal for the Dartmouth summer research project on AI 1956'

Powles J and Hodson H, 'Google DeepMind and healthcare in an age of algorithms' (2017) Health Technol 351

Price N,'AI in health care: applications and legal implications' (2017) 14(1) The SciTech Lawyer 10-13

Reddy S and others, 'A governance model for the application of AI in health care' (2019) 27(3) 2020 Journal of the American Medical Informatics Association 491, 492

Riedo M and Tormen L, 'The proposed EU Regulation on AI: A proportional risk-based approach to a civil liability regime for AI' (2021) >https://portolano.it/en/newsletter/litigation-arbitration/the-proposed-eu-regulation-on-ai-a-proportional-risk-based-approach-to-a-civil-liability-regime-for-artificial-intelligence#_ftn2< accessed 18 May 2022

Marijn Sax, 'Between Empowerment and Manipulation: The Ethics and Regulation of For-Profit Health Apps' (PhD Thesis, Universiteit van Amsterdam (UvA) 2021) 110–12

Schneeberger D, Stöger K, and Holzinger A, 'The European Legal Framework for Medical AI' (2020) IFIP 209

Schönberger D, 'Artificial intelligence in healthcare: a critical analysis of the legal and ethical implications' (2019) 27 International Journal of Law and Information Technology 171–203

Smits J M, 'What is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research' (2015) 2015/06 M-EPLI Working Paper

Spindler G, 'Roboter, Automation, künstliche Intelligenz, selbststeuernde Kfz - Braucht das Recht neue Haftungskategorien?' (2015) 31 Computer und Recht 766–776

Sunarti S and others, 'AI in healthcare: opportunities and risk for future' (2021) Gac Sanit

Theofilators K and others, 'Predicting protein complexes from weighted protein-protein interaction graphs with a novel unsupervised methodology: Evolutionary enhanced Markov clustering' (2015) 63(3) AI Med 181

Van Alsenoy B, 'Liability under EU Data Protection Law; From Directive 95/46 to the General Data Protection Regulation', 7 (2016) JIPITEC 271

Vayena E, Blasimme A, and Cohen I G, 'Machine learning in medicine: addressing ethical challenges' (2018) 15(11) PLoS Med

Zech H, 'Künstliche Intelligenz und Haftungsfragen' (2019) 5 Zeitschrift für die gesamte Privatrechtswissenschaft 198–219

Zech H, 'Liability for AI: public policy considerations' (2021) ERA Forum 147-158

Zednik C, 'Solving the Black Box Problem: A Normative Framework for Explainable AI', >https://arxiv.org/ftp/arxiv/papers/1903/1903.04361.pdf< accessed 10 April 2022

Zuiderveen Borgesius F J, 'Strengthening legal protection against discrimination by algorithms and AI' (2020) 24(10) The International Journal of Human Rights

Zuiderveen Borgesius F J and Veale M, ‘Demystifying the Draft EU AI Act’ (2021) 4 CRi 97-112

European Commission documents and websites

European Commission, ’Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises’ 2003/361/EC L 124/36

European Commission, ’Advancing the IoT in Europe’ SWD(2016) 110 final

European Commission, ’Building a European Data Economy’ COM(2017) 9 final.

European Commission, ’AI for Europe’ COM(2018) 237 final

European Commission, ’Coordinated Plan on AI’ COM(2018) 795 final

European Commission, ‘Report on the application of Directive 85/374/EEC on the approximation of the laws, regulations, and administrative provisions of the Member states concerning liability for defective products’ COM(2018) 246 final

European Commission, ‘Ethics guidelines for trustworthy AI’ (2019) >https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai< accessed 18 May 2022

European Commission, ‘Report on the safety and liability implications of AI, the IoT and robotics’ COM(2020) 64 final

European Commission, ‘White Paper on AI - A European approach to excellence and trust’ COM(2020) 65 final

European Commission, Press release, ‘Public health: Stronger rules on medical devices’, 26 May 2021 >https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2617<

European Commission, Single market and standards, ‘CE marking’ >https://ec.europa.eu/growth/single-market/ce-marking_de<

European Commission, Press release, ‘Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in AI’, 21. April 2021 >https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682< accessed 05 May 2022

European Commission, ‘Civil liability - adapting liability rules to the digital age and AI’ >https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en< accessed 19 May 2022

European Commission, ‘Commission collects views on making liability rules fit for he digital age, AI and circular economy’ (20 October 2021) > https://ec.europa.eu/growth/news/commission-collects-views-making-liability-rules-fit-digital-age-artificial-intelligence-and-2021-10-20_en< accessed 24 May 2022

Art. 29 Data Protection Working Party, ‘Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679’ (2018), WP251rev.01

von der Leyen U, ‘A Union that strives for more; My agenda for Europe’ >https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf< accessed 10 May 2022.

European Parliament documents

European Parliament, ’Report with recommendations to the Commission on Civil Law Rules on Robotics’ (2017) 2015/2012(INL)

European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for AI (2020/2014 (INL))

European Parliament, ’Resolution on a framework of ethical aspects of artificial intelligence, robotics and related technologies’ (2020) 2020/2012(INL)

European Parliament, ’Resolution on intellectual property rights for the development of artificial intelligence technologies’ (2020) 2020/2015(INI)

European Parliament, ’Public Health’ (Factsheet) > https://www.europarl.europa.eu/ftu/pdf/en/FTU_2.2.4.pdf< accessed 5 May 2022

Guidelines and Expert studies

BEUC, ‘Adapting civil liability rules tot he new digital technologies’ (6 January 2022) > https://www.beuc.eu/publications/beuc-x-2022-002_response_to_public_consultation_on_pld_and_civil_liability_for_ai.pdf< accessed 24 May 2022

Council of Europe, ’European ethical Charter on the use of AI in judicial systems and their environment’, adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3-4 December 2018)

European Commission, Report of the Expert Group on Liability and New Technologies: ‘Liability for AI and other emerging digital technologies’ (2019)

European Commission, Register of Commission Expert Groups and Other Similar Entities, ‘Expert Group on liability and new technologies (E03592)’ >https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3592&NewSearch=1&NewSearch=1a< accessed 11 May 2022

European Data Protection Board, ‘Guidelines 05/2020 on consent under Regulation 2016/679’, (2020) Version 1.1 >https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf < accessed 02 May 2022

European Group on Tort Law, ‘Principles of European Tort Law’ >http://www.egtl.org/docs/PETL.pdf< accessed 11 May 2022

WHO, Guidance 'Ethics and Governance of AI for health' (2021), >https://apps.who.int/iris/rest/bitstreams/1352854/retrieve< accessed 15 May 2022.

Blogs and other websites

Angwin J, Larson J, Mattu S, and Kirchner L, 'Machine Bias' (*ProPublica,* 2016) >https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing< accessed 10 April 2022

Bach I, 'Einführung in die Juristische Methodenlehre' (*Uni Göttingen,* 2020/2021) >https://www.uni-goettingen.de/de/document/download/83cfd1ca6a8f15427fbd6cc039250e6d.pdf/Methodenlehre%20-%20Skript%202020.pdf< accessed 23 May 2022

Bellinghausen R and Bauwens K, 'Product Liability and AI (Part 2) - The EU Commission's plans for adapting liability rules to the digital age' (*Linklaters,* 16 July 2021) >https://www.linklaters.com/en/insights/blogs/productliabilitylinks/2021/july/product-liability-and-ai-part-2-eu-commissions-plans-for-adapting-rules-to-the-digital-age< accessed 19 May 2022

Chasserieau J and Visser L, 'Digitaleurope's initial findings on the proposed AI Act' (*Digitaleurope,* 10 August 2021) > https://www.digitaleurope.org/resources/digitaleuropes-initial-findings-on-the-proposed-ai-act/< accessed 18 October 2021.

Edelmann S, '4 key benefits of applying AI to medical records' (*Healthcare Transformers,* 21 July 2021) >https://healthcaretransformers.com/digital-health/ai-improves-electronic-health-records/< accessed 05 April 2022.

EDPB, News, 'The Swedish Authority for Privacy Protection (IMY) issues an administrative fine against Klarna Bank AB after investigation' (5 April 2022), >https://edpb.europa.eu/news/national-news/2022/swedish-authority-privacy-protection-imy-issues-administrative-fine-against_en< accessed 15 April 2022.

Federal Ministry of Health, 'Driving the digital transformation of Germany's healthcare system for the good of patients' (2020) >https://www.bundesgesundheitsministerium.de/en/digital-healthcare-act.html< accessed 10 May 2022

Fichtner E, 'Cybersecurity 101: Intro to the Top 10 Common Types of Cybersecurity Attacks' (*datto,* 31 January 2022) >https://www.datto.com/blog/cybersecurity-101-intro-to-the-top-10-common-types-of-cybersecurity-attacks< accessed 21 April 2022.

Freeman R and others, 'Product liability and safety in the EU: overview' (*Thomson Reuters,* 2022) >https://uk.practicallaw.thomsonreuters.com/w-013-0379?transitionType=Default&contextData=(sc.Default)&firstPage=true < accessed 02 May 2022.

French AI Strategy Report >https://www.aiforhumanity.fr/en/< accessed 12 May 2022.

Gaumond E, 'AI Act: What is the European approach to AI?' (*Lawfare,* 4 June 2021) > https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai< accessed 18 May 2022.

German AI Strategy >https://www.ki-strategie-deutschland.de/home.html?file=files/downloads/Nationale_KI-Strategie_engl.pdf< accessed 12 May 2022.

DG CONNECT, Gabriele Mazzini, 'A European Strategy for AI' (2nd ELLIS Workshop in Human-Centric Machine Learning (YouTube recording), 10 May 2021) >https://youtu.be/OZtuVKWqhl0?t=10346< accessed 18 May 2022, at 2:52:26 et seq

McKnight W and Dolezal J, 'Healthcare Natural Language Processing' (*Gigaom,* 16 March 2022) >https://gigaom.com/report/healthcare-natural-language-processing/< accessed 05 April.

Ordish, J, Murfet H, and Hall A, 'Algorithms as medical devices' (*PHG Foundation,* 2019) >https://www.phgfoundation.org/media/74/download/algorithms-as-medical-devices.pdf< accessed 25 April 2022.

Poremba S, ‘Data Poisoning: When Attackers Turn AI and ML Against You’ (*Security Intelligence,* 21 April 2021) >https://securityintelligence.com/articles/data-poisoning-ai-and-machine-learning/< accessed 20 April 2022.

Rosenthal S and Müller-Peltzer P, ‘Künstliche Intelligenz - wer haftet, wenn ein Roboter versagt?’ (*Schürmann, Rosenthal, Dreyer,* 22 August 2019) >https://www.srd-rechtsanwaelte.de/blog/kuenstliche-intelligenz-haftung/< accessed 05 May 2022.

Strübin M, ‘AI in medical technologies: improving the lives of citizens and patients’ (2021) 543 The Parliament; Politics, Policy and People Magazine

Sveriges Radio, ’Apoteket apologizes for sharing around a million customer details to facebook’ >https://sverigesradio.se/artikel/apoteket-apologizes-for-sharing-around-a-million-customer-details-to-facebook< accessed 22 May 2022

Swedish AI Strategy Report >https://www.government.se/4a7451/contentassets/fe2ba005fb49433587574c513a837fac/national-approach-to-artificial-intelligence.pdf< accessed 12 May 2022.

Think Automation, ’The AI black box problem’ <https://www.thinkautomation.com/bots-and-ai/the-ai-black-box-problem/> accessed 10 April 2022

University of Groningen, ‘Sensitive data and medical confidentiality’ >https://www.futurelearn.com/info/courses/protecting-health-data/0/steps/39608< accessed 23 May 2022

Table of Cases

EU cases

Case C-495/10 Centre hospitalier universitaire de Besançon v Thomas Dutrueux and Caisse primaire d'assurance maladie du Jura [2011] ECLI:EU:C:2011:869

Case C-310/13 Novo Nordisk Pharma GmbH v S. [2014] EU:C:2014:2385

German Cases

BVerfG 17.5.1960 - 2 BvL 11/59 und 11/60,

BVerfGE 17.05.1960 - 11, 126

Table of Legislation

EU Legislation

Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member states concerning liability for defective products (85/374/EEC)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (2001) OJ L 11/4

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices

Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code

Proposed EU Legislation

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on AI (AI Act) and amending certain Union legislative acts (COM(2021) 206 final)

German Legislation

Bundesärztekammer, Bekanntmachungen, (Muster)-Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte, MBO-Ä 1997 in der Fassung des Beschlusses des 124. Deutschen Ärztetages vom 05. Mai 2021 in Berlin >https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Recht/_Bek_BAEK_MBO-AE_Online_final.pdf< accessed 05 May 2022

Bundesministerium für Digitales und Verkehr, 'Gesetz zum autonomen Fahren tritt in Kraft' (27 July 2021) > https://www.bmvi.de/SharedDocs/DE/Artikel/DG/gesetz-zum-autonomen-fahren.html< accessed 24 May 2022

Deutscher Bundestag, Sachstand, 'Grundzüge der Arzthaftung in Deutschland aus zivil- und strafrechtlicher Perspektive' (2021), WD 7 - 3000 - 091/21

Deutscher Bundestag, 'Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation' (2019) Drucksache 19/13438

Federal Ministry of Health, 'Driving the digital transformation of Germany's healthcare system for the good of patients' (2020) >https://www.bundesgesundheitsministerium.de/en/digital-healthcare-act.html< accessed 10 May 2022 European Commission, 'Commission collects views on making liability rules fit fort he digital age, AI and circular economy' (20 October 2021) > https://ec.europa.eu/growth/news/commission-collects-views-making-liability-rules-fit-digital-age-artificial-intelligence-and-2021-10-20_en< accessed 24 May 2022

Patientenrechtegesetz, BGBl. I 2013, 277; Bundesministerium der Justiz, 'Patientenrechte' >https://www.bmj.de/DE/Themen/VorsorgeUndPatientenrechte/Patientenrechte/Patientenrechte_node.html