The Battle between Innovation and Regulation in Digital Health Applications which use Artificial Intelligence.

Francesca Hili

Master in Transnational Law

Católica Global School of Law | Faculdade de Direito da Universidade Católica Portuguesa

Supervisor: Dr Jeanne-Pia Mifsud Bonnici

Date of Submission: 29th March 2023

The research work disclosed in this publication is partially funded by the Endeavour Scholarship Scheme (Malta). Project part-financed by the European Social Fund- Operational Programme II – European Structural and Investment Funds 2014-2020 "*Investing in human capital to create more opportunities and promote the well-being of society".*

I wish to express my sincere thanks and appreciation to my supervisor Dr Jeanne-Pia Mifsud Bonnici for her guidance and support throughout the research and writing process. I am also grateful to my family for their moral support, especially to my father and grandfather for their help in proofreading this thesis. Lastly, I would like to express my gratitude to Vincenzo for always being a source of encouragement and motivation.

Abstract

The use of AI in the digital health sector has been rising consistently over the past years and it is common for people to make use of digital health applications which use AI for various health and wellbeing reasons. Furthermore, innovation in relation to AI is high in the present times and also within the digital health sector. This thesis aims to analyse the existing regulatory environment which regulates these applications with the aim of understanding whether a balance is reached between innovation and protection of users. Regulation should not deter innovation, and neither should it fail to protect users from risks prevalent within AI in the digital health market. This is why ideally a balance should be reached. The research will be based on doctrinal analysis and an interdisciplinary literature review to explain the issues which arise from the use of AI within digital health applications.

Regulation affects innovation in relation to technology in multiple ways and the regulator faces issues such as the pacing problem and difficulty to maintain regulatory connection within the fast-moving pace of technology. The research sets out the issues relating to the use of AI in digital health in relation to three topics: the classification of AI as a medical device, sourcing and processing of health data, and transparency and accountability in AI. Any existing or proposed EU legislation, namely the Artificial Intelligence Act, the Medical Devices Regulation, the General Data Protection Regulation and the European Health Data Space Regulation, which regulate digital health applications in relation to these issues were analysed in order to understand the extent of applicable provisions. These provisions were then analysed to understand their effects on innovation versus user protection and it was concluded that the current regulatory environment does not reach a balance. It favours innovation in some instances through legal certainty and deters both innovation and user protection in other instances.

Digital Health Applications – Regulation and Innovation – Artificial Intelligence as a Medical Device – Health Data – Transparency

Abbreviations

Artificial Intelligence	AI
Artificial Intelligence Act	AI Act
Court of Justice of the European Union	CJEU
European Data Protection Board	EDPB
European Health Data Space	EHDS
European Union	EU
General Data Protection Regulation	GDPR
Malta Digital Innovation Authority	MDIA
Medical Devices Regulation	MDR
Natural Language Processing	NLP
Small and Medium Enterprises	SMEs
United States of America	USA

Table of Cases

EU:

BIOS Naturprodukte GmbH v Saarland (C27/08)
Chemische Fabrik Kreussler & Co. GmbH v Sunstar Deutschland GmbH, formerly John O. Butler GmbH (C308/11)
Hecht-Pharma GmbH v Staatliches Gewerbeaufsichtsamt Lüneburg (C140/07)
Syndicat national de l'industrie des technologies médicales (Snitem) and Philips France v Premier ministre and Ministre des Affaires sociales et de la Santé (C329/16)

USA:

Dinerstein v. Google, LLC et al, Chicago, United States District Court Northern District of Illinois (19-4311)

Table of Legislation

EU Law:

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence COM/2021/206 (Artificial Intelligence Act)
Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space COM/2022/197 (European Health Data Space Regulation)
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Medical Devices Regulation)
Treaty on the Functioning of the European Union

Maltese National Law:

Chapter 591 of the Laws of Malta, Malta Digital Innovation Authority Act
Chapter 592 of the Laws of Malta, Innovative Technology Arrangements and Services Act

Guidelines:

Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, February 2018
Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, October 2019

Table of Contents

Introduction

'Digital health' is an umbrella term which can be difficult to define. Sonnier described digital health as '*the convergence of the digital and genomic revolutions within health, healthcare, living, and society'.*[1] The European Users' Forum defines digital health as '*healthcare practices supported by electronic processes and communication. It includes a wide range of services and information technology such as electronic medical records, telemedicine, evidence-based medicine, consumer health informatics etc'.*[2] Sometimes, various terms are also used interchangeably although not all of them may refer to the same thing; digital health, e-Health, mHealth. The World Health Organization defines e-Health as '*the use of information and communication technologies for health'*[3] and this is an umbrella term very similar to digital health whereas mHealth (mobile health) refers specifically to the practice of health through mobile phones. These explanations and definitions highlight how broad the term digital health is and how difficult it can be to define it.

For the purposes of this thesis, the author will be referring to digital health applications which use artificial intelligence ('AI'). The term applications is being used to refer to software which performs specific tasks or functions. This will generally include any applications which operate within the digital health sector, and which use AI to provide a digital health service to users. It may include applications which assist in checking symptoms and diagnosis, applications which provide therapeutic services through a platform and applications which assist users in managing disease, to give a few examples. This excludes applications used for administration of users within a hospital or clinic environment as will be explained further in Chapter 1.

The main aim of this thesis is to answer the following research question:

> *Does the present regulatory environment achieve a balance between innovation in digital health applications which use AI and the protection of users?*

---

[1] Paul Sonnier, *Definition of Digital Health, Etymology & Plurality of the Term*, Published on April 12, 2020 <https://www.linkedin.com/pulse/definition-digital-health-etymology-plurality-term-paul-sonnier/> last accessed 26th November 2022

[2] <https://www.eupatient.eu/policy/Policy/eHealth/#:~:text=Digital%20health%20refers%20to%20healthcare,%2C%20consumer%20health%20informatics%2C%20etc.> last accessed 26th November 2022

[3] European User Forum Position Paper on eHealth <https://www.eu-patient.eu/globalassets/policy/ehealth/epf-final-position-paper-on-ehealth_19december2016.pdf> last accessed 26th November 2022

To be able to answer this question, this thesis strives to analyse both existing EU legislation and proposed EU legislation which govern digital health applications in the present market in order to assess the effects the current regulatory regime has on the operations of digital health applications which use AI. The assessment will be limited to legislation which affects users, namely, the General Data Protection Regulation ('GDPR'), the proposed Artificial Intelligence Act ('AI Act'), the proposed European Health Data Space Regulation ('EHDS') and the Medical Devices Regulation ('MDR'). It is noted that other legislation whether codified or in proposal form exists which may also contribute to regulating these digital applications. However, due to the limitations of this thesis, these will be excluded from the discussion for the purposes of this research.

Currently, there are various legislations which target different areas of the operation of digital health applications indirectly, but none that tackle the regulation of digital health applications directly. Therefore, compliance may be complicated because the applications need to comply with various parts of different legislation whilst different regulators have varied levels of power to enforce. The proposed EU law and the EU's Digital Agenda[4] imply that the near future will hold increased regulation. However, it is unclear what effect this increased regulatory oversight may have on the digital health market.

The term regulatory oversight is being used within this thesis to refer to promulgated or proposed EU legislation and includes any power delegated to bodies to enforce such legislation and interpret such legislation through the publishing of official guidelines, for example. Therefore, this term is being used in order to infer the broad implications of regulation as enhanced and interpreted through guidelines, standards and procedures adhered to within the market and considered to be the market norm.

Furthermore, the effects of regulation on innovation will be studied to be able to answer the main research question set out above. It is important to assess how regulation affects innovation in order to be able to determine the potential effects the regulation of digital health applications might have on innovation within this sector.

[4] <https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe> last accessed 17th November 2022

The research methods used to analyse the regulatory environment is based on doctrinal analysis with the analysis focusing on codified legislation, proposed EU legislation, compromise texts for proposed EU legislation, case law and legal literature.

First, an analysis of existing legal literature regarding the relationship between law and innovation is undertaken with the intention of understanding the effects that the regulatory environment has on innovation. This is the first step in building this thesis since the focus is on analysing the effects of the existing regulatory environment. The second step sets out the risks which AI poses to users of the digital health market. Here, an interdisciplinary literature review will be undertaken with a focus on AI and any legal risks associated with its use in digital health to understand what risks digital health users face. Therefore, the focus is shifted onto the user as opposed to the legislation. Finally, doctrinal analysis of the applicable legislation falling within the scope of this thesis is undertaken in order to establish the existing regulatory environment for AI in digital health.

1. The Relationship between Regulation and Innovation

1.1. Defining Innovation and Regulation

This section will delve into the effects regulation can have over innovation. This will establish what innovation and regulation will refer to for the purposes of this thesis and will set forth criteria which will be used to analyse the current regulatory environment for digital health applications which use AI.

1.1.1. Innovation

Innovation generally refers to the use of a new idea, method or device, to offer new or improved goods or services. It may be disruptive or incremental wherein disruptive innovation replaces the previously existing products or processes completely whilst incremental innovation improves existing products and processes through minor improvements.[5]

Innovation is invested in by different people or entities and for different reasons. Investors within the digital health space might invest in innovation which aims to make healthcare more efficient and accessible but commercialisation of the product or service and the potential for profits is also an important part of the decision to invest. For a company to be profitable, their innovative product or service must be accepted by the users they target and thus, diffusion of innovation[6] is very important.

Within this thesis, innovation will refer to a '*novel idea'* which is successfully diffused in the market.[7] Innovation is not necessarily the first invention of a specific product or service but the first successful attempt to carry it out in practice and launch it in the relevant market.[8] For the purposes of this thesis, the author will also be assuming that innovation means technological developments within digital health which impacts users directly and does not refer to any innovation arising from management, organization or marketing processes. This is because this thesis will assess whether the current existing and proposed legislation protects the rights and

[5] Jacques Pelkmans, Andrea Renda, *How can EU Legislation Enable and/or Disable Innovation*, European Commission, July 2014.
[6] E.M Rogers proposed his theory on the diffusion of innovation in 1962 and it explains how an invention diffuses through a social system over time and in steps.
[7] Anna Butenko, Pierre Barouche, *Regulation for Innovativeness or Regulation of Innovation, Law,* Innovation and Technology, 2015 7(1) p. 54.
[8] Ibid.

freedoms of users in relation to digital health and innovation arising from management, organization or marketing processes tend to pose less severe risks to users.

Digital health is in itself an innovation of the traditional health services sector since it consists of new methods for providing health services which are traditionally provided by doctors without the use of digital tools. Innovation within the digital health services sector may be seen in applications which assist doctors in providing health services such as software which screens x-rays[9] and compares them to datasets in order to arrive at a diagnosis. Such software includes an AI algorithm which continues learning and improving with every dataset analysed. Other innovative digital health applications bypass the need for doctors and advise users directly, such as applications which diagnose the probability of skin cancer through a photo.[10]

1.1.2. Regulation

Regulation is the '*sustained and focused attempt to alter the behaviour of others according to standards or goals with the intention of producing a broadly identified outcome, which may involve mechanisms or standard-setting, information gathering and behaviour modification'.*[11] Thus, regulation within the health sector aims to produce the broadly identified outcome of ensuring safe services for users.

Regulation may be narrowly interpreted to refer to the promulgation of legislation or more generally to also include all actions taken by agencies or entities to control and influence products or services which affect society.[12] Top-down regulation normally includes a formal legislation which is promulgated by a regulator and applies to specific regulatees. In certain instances, bottom-up regulation may also occur where industry practices form, and although informal those operating

[9] One example is CheXneXt which is an algorithm trained to evaluate chest x-rays for a multitude of potential illnesses <https://med.stanford.edu/news/all-news/2018/11/ai-outperformed-radiologists-in-screening-x-rays-for-certain-diseases.html> last accessed 19th March 2023

[10] One example is AI Dermatologist, an application which uses an AI algorithm to distinguish between benign and malignant tumours based on oncology rules <https://ai-derm.com/> last accessed 19th March 2023

[11] Julia Black, *What is regulatory innovation?*, Regulatory Innovation: a Comparative Analysis (Edward Elgar Publishing 2005)

[12] Butenko (n7) p. 56

within that industry or market adhere to them without question and there is a much less clear distinction between regulator and regulatees.[13]

Brownsword describes how normative regulation is normally aimed at the present possibilities which may be incompatible with technology and the new possibilities it is constantly creating. On the other hand, if the regulatory environment is treated as a '*regulated sphere of possibility'* which '*engages with spheres of possibility but in ways that restructure those regulatory spaces and redefine what is and is not possible'* this will change the impact of regulation on technological innovation.[14] This would mean that laws would be seen as one part of an overarching regulatory environment where technological management is also part of it. Practically, this would translate into regulators defining what is possible instead of regulating belatedly what regulatees can or cannot do.[15]

The terminology used to analyse and describe regulation includes, '*instrument choice, regulator's toolkit* [and] *policy tools'* and therefore, regulation can be considered the technology of governance.[16] Within normative regulation, the form of regulation promulgated makes a difference in impact and this may be seen by a simple example; EU Directives need to be implemented into national law and thus, some fragmentation may occur whilst EU Regulations apply directly to all EU member states thus reducing the risk of fragmentation significantly. Regulators aim to set standards, prohibit actions, establish licensing procedures, and set requirements for regulatees.[17]

For the purpose of this thesis, regulation will mainly refer to enacted and proposed legislation and any guidelines, standards or procedures emanating from such.

1.2. The Challenges of Regulating Innovation

Many studies have been undertaken on innovation ranging from studies probing the conditions for successful innovation, to studies on the sources of invention and the diffusion of innovation within

[13] Roger Brownsword, *Law, Technology and Society, Re-Imagining the Regulatory Environment* (Routledge 2019) pg 43
[14] Ibid. p. 40
[15] Ibid. p. 8
[16] Jonathan B. Wiener, *The Regulation of Technology and the Technology of Regulation*, Technology in Society, 2004, 26 p. 484
[17] Brownsword (n13) p. 5

society. However, these studies are not linked; relate to innovation within different sectors; and can be difficult to integrate to achieve a better theoretical framework.[18]

The relationship between regulation and innovation has also been studied from two main perspectives: that of law and economics focusing on '*the mechanisms which stimulate innovation in a market economy'* and from the perspective of law and technology focusing on '*the regulation of innovations'*.[19] Literature based on the law and economics perspective tends to assume that the innovation is inherently positive and regulation should focus on correcting market failures in order to enable the innovation to prosper.[20] Law and technology based literature tends to assume that technological developments are a constant and will naturally happen over time and thus may fail to explore the way regulation affects this development.[21]

Regulating innovation, especially technological innovation, gives rise to the so-called '*pacing problem'*. This refers to the issues which arise when technology develops faster than the law updates itself. Regulation will need to manage newly arisen risks, assess the application of existing laws, and adapt new regulations as a result of the technological changes.[22] This is described by Brownsword as the challenge of regulatory connection.[23]

It is very hard for any technology to fall within a complete legal void, since many aspects of the business will fall within parameters of some existing legislation such as that regulating liability, competition or data privacy.[24] However, certain aspects of the technology which create specific ethical and moral issues may not be targeted by any regulation. This could be due to the fact that before an innovation is diffused into the market, issues which need to be legally regulated may not be foreseen.

Furthermore, innovation needs to be diffused within society to be successful. Therefore, a timing issue arises. It is difficult to foretell the issues which will arise from a proposed or newly launched innovation. However, if an innovation successfully diffuses in society, then it is also difficult to

[18] Richard R. Nelson, Sidney G. Winter, *In Search of Useful Theory of Innovation*, Research Policy, 1977, 6(1) pg 46
[19] Butenko (n7) p. 53
[20] Ibid. p. 63
[21] Ibid. p. 69
[22] Lyria Bennett Moses, *How to Think about Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target*, Law, Innovation and Technology, 2013, 5(1) p. 7
[23] Roger Brownsword, *Rights, Regulation and the Technological Revolution*, Oxford University Press, 2008, Ch 6
[24] Butenko (n7) p. 68

change things retrospectively. Should the regulator intervene early in a negative manner, this will highly discourage innovation. Should the regulator send positive signals early, such as preferential taxation or subsidies, this will then encourage innovation for that specific invention. Early intervention by the regulator is very risky, since there will be a lack of information and thus, it is very difficult to accurately predict what the issues requiring regulation will be. Intervening at a later stage, may have a better result since inventions which do not diffuse successfully will be naturally eliminated and a regulatory assessment based on facts and evidence may be conducted.[25]

Furthermore, technology specific regulation tends to have a shorter lifespan. Technology evolves quickly and the use of technology changes and thus a very specific legislation will not be able to stay relevant all throughout these changes. Technology-neutral regulation which includes principles to regulate technology but is not specific to one sector of technology is more sustainable and future-proof.[26] The European Commission has defined technology neutrality to mean regulation which '*neither imposes nor discriminates in favour of the use of a particular type of technology'*.[27] One example of technology neutral regulation is the GDPR where the law is applicable to all data processing within a commercial context and which has managed to achieve a compliance upheaval in many countries.

Brownsword and Goodwin[28] have argued that regulators have four challenges to face in order to create the right regulatory environment.

1. The first challenge is that of prudence and precaution in the face of prevalent uncertainty in new technology. How can the risks be balanced against the benefits of the technology?
2. The second challenge relates to regulatory legitimacy. Have stakeholders and the public participated in the debate leading up to the regulations?
3. Thirdly, there is the challenge of whether the chosen regulatory strategy achieves balance. Problems can arise if resistance is shown by the regulatees or if there are external disruptive factors.

[25] Ibid. p. 73
[26] Ibid. p. 75
[27] <https://eur-lex.europa.eu/EN/legal-content/summary/supporting-telecommunications-networks-and-digital-service-infrastructures-across-europe.html> last accessed 4th March 2023
[28] Roger Brownsword, Morag Goodwin, *Law and the Technologies of the 21st Century*, Cambridge University Press, 2012, Ch 3

4. And the final challenge is of regulatory connection. This challenge may be split into three parts which starts with making a regulatory connection; continuing to stay connected as the use of the technology spreads; and getting reconnected once the technology use changes.[29]

These challenges will be discussed in Chapter 5 when analysing whether the current regulatory environment is the ideal regulatory environment to balance between innovation and regulation of user risks.

[29] Ibid.

2. AI in Digital Health Applications

As discussed previously, digital health is an innovation of the traditional health sector. The use of AI in digital health applications allows for further innovation of services which may be provided under the digital health sector, but it also introduces specific risks related to such AI use.

2.1. What is AI?

AI is the science of developing intelligent computers.[30] It includes different techniques with some being more suited to use in healthcare than others. Machine learning is a subset of AI and consists of a set of algorithms which allow software to learn from datasets. This can be done at different levels of complexity. Machine learning uses different approaches to learn from the training datasets and may be categorized into supervised learning, unsupervised learning and reinforcement learning. The former two require labelled and unlabelled datasets respectively whilst reinforcement learning learns through interaction. Engineers are sometimes faced with the problem of insufficient labelled data for supervised learning and to overcome this in an inexpensive manner, they may opt to incorporate a model already trained on another similar dataset before proceeding with training on the limited labelled data available to them.[31] Essentially, the AI will build assumptions based on patterns found within the datasets.[32] Therefore a machine learning algorithm is an algorithm programmed to learn to do a task.[33]

Deep learning involves multiple layers of neural network models that mimic the human brain to predict outcomes. NLP refers to the way a computer understands the meaning of written words and can be tricky since nuance, context and interpretation add necessary information. [34]

AI is often referred to as a 'black box' due to its self-learning attributes. This means that humans find it difficult to understand how variables are processed to reach a final prediction. Interpretable

[30] Urs J. Muehlematter, Paola Daniore, Kerstin Vakinger, *Approval of AI and machine-learning based medical devices in the USA and Europe (2015-20): A Comparative Analysis*, Lancet Digital Health 2021, 3(3), p. 195
[31] Yap Jia Qing, Ernest Lim, *A Legal Framework for Artificial Intelligence Fairness Reporting,* Cambridge Law Journal, 2022 81(3) p. 616
[32] Michael Matheny and others, *AI in Health Care, The Hope, The Hype, The Promise, The Peril*, NAM Special Publication Washington DC, 2019 p. 15
[33]<https://medium.com/predict/what-is-an-ai-algorithm-aceeab80e7e3> last accessed 06.01.2023
[34] Thomas Davenport, Ravi Kalakota, *The Potential for AI in Healthcare*, Future Healthcare Journal 2019 6(2) p. 94-95

AI models are possible. However, most models are not designed with interpretability in mind, and this hasn't been challenged much to date. The focus is put on the fact that AI has a higher level of accuracy when compared to humans and their margin for error. Not enough focus is put onto whether the same level of accuracy could be reached with better transparency.[35]

These characteristics of AI, its self-learning attributes and its reliance on labelled or unlabelled datasets respectively need to be kept in mind when discussing the regulatory framework.

2.2. AI in Digital Health: Risks and Issues

It has been proven that AI outperforms doctors in fields such as dermatology and radiology due to the AI's ability to process patterns which might not be easily identifiable to humans.[36] Beneficiaries of AI in digital health may range from user to doctors or researchers. Machine learning can be found in applications which track health such as a fertility tracker for women which give predictions of their cycle.[37] Machine learning can also assist doctors in reading medical images or for early cancer detection. NLP might also be present in any chatbots used in such applications. Researchers may also benefit from AI's prediction of cancer based on genetics and any other variables to name a few examples.[38] All these possibilities fall under the umbrella term 'digital health' which differs significantly from the traditional health market in many ways.

2.2.1. Medical Devices

Normally, regulators have power to limit medical devices[39] entering the health market. However, in digital health it's very difficult to regulate applications entering the market. Digital health applications may update themselves through self-learning without necessarily being obliged to release an explicit update and this means that a regulator would have even less control.[40] Effective

---

[35] <https://hdsr.mitpress.mit.edu/pub/f9kuryi8/release/8> last accessed 06.01.2023

[36] Anmol Arora, *Conceptualising AI as a Digital Health Innovation: An Introductory Review, Medical Devices: Evidence and Research*, Auckl 2020, 13 p. 224

[37] Flo is a fertility tracker which uses neural networks to predict ovulation and period dates <https://flo.health/faq/accuracy#:~:text=We%20use%20artificial%20intelligence%2C%20an,up%20to%2054.2%25%20more%20accurate.> last accessed 28th March 2023

[38] Matheny (n32) p. 61

[39] This is done through the MDR - Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices.

[40] Jeffrey David Iqbal, Nikola Biller-Andorno N, *The Regulatory Gap in Digital Health and Alternative Pathways to Bridge it*, Health Policy and Technology, 11(3) 2022 p. 1-2

regulatory oversight must exist in order to audit the safety and efficiency of AI at constant intervals.[41]

Furthermore, the traditional understanding of a medical device needs to be adapted to include the characteristics of applications. Presently, lifestyle and wellbeing applications are classified separately then software as a medical device with the latter being afforded more regulatory freedom. However, the use of AI in both type of applications within the digital health market may have similar risks to users.

2.2.2. Health Data

The present advances of AI within digital health may be attributed to the vast amounts of health data generated by users through technologies such as wearable devices and electronic health documentation. However, there are still barriers to health data availability especially when taking into consideration the vast amounts of data required to train AI accurately. Furthermore, there must be continued availability of data with potentially bigger and more updated datasets in order to continuously improve the AI.[42]

Building health datasets may prove to be problematic given the sensitive nature of health data. Wearable internet of things devices give companies a limited insight into a limited window of data and such data is not often accessible to other researchers.[43] Web scraping will provide limited results given the private nature of the data and to date, there are only 3455 open sourced health datasets available on data.world.[44]

It is important to note that the purpose for collecting this data is normally for personal health reasons and not to train AI and the secondary use of the collected personal data gives rise to issues.[45] This may also create data bias since the sources of data may under-represent a certain race, age or sexual orientation and there is less control over the dataset.[46] Training an AI on a purposefully

[41] Effy Vayena and others, *Machine Learning in Medicine: Addressing Ethical Challenges*, PLoS Med, 15(11), 2018
[42] Yuri M Aung and others, *The Promise of AI: A Review of the Opportunities and Challenges of AI in Healthcare,* British Medical Bulletin, 2021, 139 p. 8
[43] Jane Thomason, *Big Tech, Big Data and the New World of Digital Health,* Global Health Journal, 2021, 5 p. 166
[44] <https://data.world/datasets/health> last accessed 3rd February 2023
[45] Matheny (n32) p.16-17
[46] Ibid. p. 20

sourced dataset and locking the algorithm may help solve this issue but the lack of evolution of the AI due to locking forgoes much of its value.[47]

Furthermore, even if data collection for the purposes of AI were to be the primary purpose, within health AI, the data collector usually does not know what data is necessary and thus cannot limit data collection to the necessary. This would in turn breach the data minimization principle in the GDPR. The AI will be created for the purposes of creating specific predictions and require large and representative datasets to produce accurate outcomes.[48] The predictions given by an AI depends on the quality of the training data fed to it, the data which users feed into the system and how any algorithms are designed to process or ignore any input data. Thus, this includes lots of variability.[49] Furthermore, sensitive inferences may be made from health data including inferences about family members and this is an issue which needs to be taken into consideration.

Therefore, concerns may be raised in relation to the sourcing of the training datasets, secondary use of data to train AI and the resulting issues related to bias, consent, anonymization and inferences in relation to purposefully sourced data.

2.2.3. Transparency and Accountability

Transparency and accountability have been introduced as data protection values through the GDPR but they were not codified with AI in mind. Transparency as a value also needs to be defined specifically for the purposes of the AI regulator. Due to AI's capability to recognize patterns which humans are not capable of noticing, the use of the term 'black box' in relation to AI is given a pejorative connotation but the opacity of AI systems and algorithms enhances this pejorative view.

On the other hand, if AI is expected to explain every action taken, this would limit the innovative capacity of AI. Instead, the focus should be on sustainable versions of transparency which allow for external audit and oversight without limiting the innovative capacity of AI as for example, transparency of the training data and of the system structure and logic.[50]

[47] Glenn Cohen and others, *The EU AI Strategy: Implications and Challenges for Digital Health*, Lancet Digital Health 2020, 2, p. 377
[48] Arora (n36) p. 226
[49] Cohen (n47) p. 378
[50] Matheny (n32) p. 191

Opacity is a cause for concern, but full transparency might also be a cause for concern since it will have negative impacts on innovation. A feasible option might be to have AI provide legally operative explanations such as answering questions about the weight given to different factors.[51] The difference here would be that an explanation would allow a human to '*determine the extent to which a particular input was determinative or influential on the output'*[52] in the same way that a judge may be asked to provide an explanation of the decision taken in some jurisdiction or in the same way an individual may have to explain his/her actions in court in order to determine whether such actions were undertaken knowingly, recklessly, negligently or innocently.[53]

Similarly, accountability is ill-defined for AI when the training data used may be interconnected and include probabilistic algorithms and open-source components.[54] Furthermore, within the health sector, the focus is traditionally on the health professional and the patient. Trust is built through the relationship between the parties. The health professional explains the suggested treatment plan to the patient but the patient has the right to refuse certain treatment and thus, the decision making is shared between the parties.[55] For AI in digital health, there is no similar trust being formed because it is often unclear how the output is created and there are no obligations on the developers to be held accountable for the algorithms they create. Furthermore, since AI may be self-learning, it further complicates the issue of accountability since the developer himself/herself may not be able to fully deduce the logic which led to the output.

To date, these values have not been specifically adapted to AI through codified legislation and thus, current digital health applications are not bound by specific accountability and transparency obligations except for those under data protection legislation, where applicable.

---

[51] Finale Doshi-Velez and others, *Accountability of AI Under the Law: The Role of Explanation*, Working Draft <https://doi.org/10.48550/arXiv.1711.01134> p. 13
[52] Ibid. p. 9
[53] Ibid. p. 11
[54] Cohen (n47) p. 378
[55] Helen Smith, *Clinical AI: Opacity, Accountability, Responsibility and Liability*, AI & Society, 2021, 36 p. 540

3. The Current Legislative Framework

Digital health applications are currently operating in a market where existing legislation regulates different parts of the business, but no specific legislation regulates the digital health business directly. The EU's digital agenda means that there are also various legislations at proposal stage which may impact digital health applications once promulgated, including legislation aimed at regulating AI. The current regulatory approach is resulting in fragmented legislation, with many compliance obligations arising from different legislations and thus being subject to enforcement by different regulators. For digital health applications, both the USA and EU have opted to use the existing medical device classifications instead of creating a specific category and this means that only digital health applications which fall within the parameters of such a classification are regulated.[56]

This chapter will assess how the issues highlighted in Chapter 2 are targeted by any existing or proposed EU legislation, if at all. For any proposed EU legislations, the main reference will be the official proposal text published by the European Commission. However, references may also be made to any proposed compromise texts where such information is available publicly in the interest of assessing the impact such changes may have if codified within the final text of the law.

The analysis will be structured under four sub-headings: classification of AI, health data, transparency and accountability, and regulatory oversight. This will allow the analysis of the applicable regulation to focus on assessing how robust regulation is in relation to the issue of classifying AI as a medical device, sourcing and processing health data for AI in digital health, transparency and accountability of AI and the role of regulatory oversight.

[56] Iqbal (n40) p. 3

3.1. Classification of AI

3.1.1. AI Act

The AI Act[57] defines an AI system to mean '*software that is developed with one or more techniques and approaches listed in Annex I[58] and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations or decisions influencing the environments they interact with'.*[59] This definition has been narrowed within a published compromise text to refer to '*systems developed through machine learning, logic and knowledge based approaches'.*[60] This removes the direct reference to software and deletes Annex 1 in an attempt to clarify between traditional software and AI systems.[61]It continues on to classify AI into three categories according to risk: prohibited systems, high risk systems and minimal risk systems.

Digital health applications which use AI will classify as high-risk if the *'AI system is intended to be used as a safety component of a product or is itself a product covered'* by other EU legislation and is subject to specific EU legislation such as the MDR or if it is listed in Annex III of the AI Act.[62] Health is not directly listed as a high-risk system under Annex III and there have been ongoing discussions to amend this. In fact, the European Parliament has proposed adding '*systems used for emergency healthcare patient triage* and *systems used in making decisions on the eligibility for health and life insurance'* to the high-risk AI category.[63]In fact, in a compromise text published in November 2022, AI models which classify emergency calls or emergency healthcare patient triage were added. However, digital health has not been added as a separate section within Annex III and thus, this will not fully remove any existing ambiguity.[64]

High-risk AI will need to comply with various compliance obligations established in Chapter 2 of the AI Act which include the establishment and implementation of a risk management system, data governance rules for data sets and training models, transparency, record keeping and technical

[57] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence 2021/0106 (COD) ('AI Act')
[58] These include machine learning approaches, logic and knowledge-based approaches and statistical approaches.
[59] AI Act Art 3(1)
[60] Compromise text 14954/22, 25th November 2022 (Interinstitutional File: 2021/0106(COD) p. 71
[61] Ibid. p. 5
[62] AI Act Art 6
[63] Ibid. Explanatory Memorandum 37
[64] Compromise text (n60) p. 198-200

documentation obligations, human oversight and accuracy, robustness, and cybersecurity. This means that any digital health application classified into the high-risk category will be obliged to comply with extensive provisions.

3.1.2. MDR

Medical devices are traditionally heavily regulated to safeguard vulnerable people's health. For example, under the MDR[65], medical devices may only be placed on the market once they're considered safe and effective and the product must be closely observed to ensure no risks emerge.

The overall purpose of the MDR is to define and classify medical devices in order to increase safety and efficiency in the European market. Software may be considered a medical device in specific circumstances only.[66] Since AI algorithms are part of the software of an application, we can conclude that AI algorithms may be classified as medical devices in some specific circumstances.

Under the MDR, a medical device includes any software which is

> *'intended by the manufacturer to be used, alone or in combination, for human beings, for one or more… specific purposes… and which does not achieve its principal intended action by pharmacological, immunological or metabolic means in or on the human body, but which may be assisted in its function by such means'.*[67]

This means that a software which is intended to be used for one of the specific medical purposes set out in the MDR, will be considered as a medical device.[68] The specific purposes are listed in an exhaustive list and include:

- *'diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,*
- *diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,*
- *investigation, replacement, or modification of the anatomy or of a physiological or pathological process or state,*

[65] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices ('MDR')
[66] Ibid.
[67] Ibid. Art 2
[68] Ibid. Recital 19

- *providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations'.*

The MDR does not define software, and a guidance document was issued by the Medical Device Coordination Group[69] to clarify. The guidance document defines '*software* as a *set of instructions that process input data and create output data. Medical device software* is also defined to mean *software that is intended to be used, alone or in combination, for a purpose as specified in the definition of a 'medical device' in the medical devices regulation…'*[70]

The MDR clarifies in recital 19 that software for general purposes even if intended for a lifestyle or well-being purpose will not be considered a medical device. This shows the limited intention behind the legislation. The regulator wanted to divide applications into two categories with those which do not fall under the medical device classification being considerably less regulated. It is important to note that applications meant for lifestyle or well-being purposes, and which do not fulfil the criteria to be considered a medical device, might still pose the same or similar risks to users depending on the exact use of the application.

Furthermore, such applications, although not developed for a medical purpose, might still be used by medical professionals when treating users such as for example, a doctor may use the data created by a fitness tracker to assess the heart health of an individual. However, if such an application is not considered a medical device, questions of reliability of the data may come into play since there is no oversight over how efficiently the device works.[71]

Classification may be problematic given that the manufacturer has some leeway to define its intended use to its advantage. The guidance document clarifies that software which does not '*perform an action on data, or… an action beyond storage, archival, communication, simple search* [or] *lossless compression'*[72] is not considered a medical device. This was confirmed by the Court of Justice of the EU ('CJEU') in *Snitem and Philips France* where the software in the case was not found to be a medical device because it was intended for the sole purpose of archiving,

[69] Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, October 2019
[70] Ibid.
[71] Trix Mudler, *The Role of Law in Protecting Personal Data Generated by Health Apps and Wearables,* University of Groningen, 2022 p. 138-139
[72]Guidance on Qualification and Classification of Software (n69) p. 8

collecting and transmitting data within a medical context.[73] The CJEU has also clarified in multiple judgments that a medical purpose covers an object intended by the manufacturer to be capable of restoring, correcting, or modifying physiological functions in natural persons.[74]

The guidance document does not specify anything about well-being or lifestyle applications and thus, the distinction between medical purpose and lifestyle and well-being purpose is left to be made by the manufacturers by default; if the software is not a medical device based on the intentions of the manufacturers, then it will fall into an unregulated category for the purposes of the MDR.[75]

Furthermore, the flexibility given to manufacturers to define their intended use, reduces the MDR's efficacy and applicability in relation to digital health applications. Any national initiatives taken by member states may partly remedy this, but this will be a fragmented effort.

3.2. Sourcing and Processing Health Data

3.2.1. GDPR

The GDPR[76] prohibits the processing of '*special categories of personal data* unless specific exceptions apply. *Special categories of personal data* refer to *personal data revealing racial or ethnic origin…the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person*, [and] *data concerning health or data concerning a natural person's sex life or sexual orientation'.*[77] Therefore, for GDPR compliant data processing, an application needs to rely on one of these exceptions. Such processing needs to be compliant in two instances; whilst sourcing data for training the AI algorithms, and for data processed through use of the application by users.

The GDPR also enshrines the principle of purpose limitation wherein it states that personal data must be collected for purposes which are specified and explicit.[78] However, for digital health

[73] CJEU C329/16, Snitem and Philips France, 2017
[74] CJEU C140/07, C27/08, C308/11 from Lincoln Tsang and others, *The Impact of AI on Medical Innovation in the EU and US*, Intellectual Property & Technology Law Journal, August 2017
[75] Guidance on Qualification and Classification of Software in Regulation (n69)
[76] 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 ('GDPR')
[77] Ibid. Art 9(1)
[78] Ibid. Art 5(1)(b)

applications which use AI, it may be difficult to communicate the purposes for processing to the users in a clear, easily readable format, since for data processed by AI and used for machine learning it can be difficult to foresee and articulate the extent of the processing. This may be further exacerbated through the digital platform business model which relies on the ability to re-purpose and cross link data, and which may be relied on by certain digital health applications. This opacity may emanate from corporate secrecy, technical illiteracy relating to algorithmic codes and from advanced AI algorithms which can escape the understanding of those with specialised training.[79]

Furthermore, according to this principle, data may not be '*further processed in a manner that is incompatible with those purposes'*.[80] This means that secondary use of health data is in breach of the GDPR unless such secondary use was explicitly included into the purpose for processing and communicated to the data subjects as such. On the same topic, Google has been sued in a class action in the USA in *Dinerstein vs Google LLC*[81] wherein the plaintiff argues that although the data was shared for research purposes to train AI, and such sharing was based on the patient's consent, Google's business model relies on collecting huge amounts of data. This means that Google could re-identify the anonymized data shared. No such cases have been brought before EU courts to date. However, this highlights how sensitive sourcing health data for training datasets is.

It is important to note that within the context of digital health applications, a fine line exists between personal data and special categories of personal data. Certain personal data (such as dietary, sleep or sport habits) is not directly related to health and as such cannot be considered a special category of personal data. However, from this personal data, inferences related to health or other special categories of personal data such as religion may be made.[82] In fact, the European Data Protection Board ('EDPB') has clarified that '*data concerning health'* may be derived from sources such as medical history, information which reveals the state of health, information gained through questions related to health and information that becomes health data through a specific context such as travelling during the Covid-19 pandemic.[83]

---

[79] Luca Marelli and others, *Fit for purpose? The GDPR and the Governance of European Digital Health*, Policy Studies, 2020 41(5), p. 453-454
[80] GDPR Art 5(b)
[81] 19-4311 - Dinerstein v. Google, LLC et al, Chicago, United States District Court Northern District of Illinois.
[82] Marelli (n79) p. 455
[83] Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak Adopted on 21 April 2020

Moreover, should the data be processed on the basis of consent for the purposes of training AI, this becomes tricky since consent may be revoked. However, once data has been added to a dataset which is fed to an AI, it may not be technically possible to delete such data.

Therefore, one can conclude that although the GDPR works well in protecting personal data, there have been no adaptations made to personal data being processed by AI.

3.2.2. AI Act

High-risk AI systems which use training datasets are required by the AI Act to meet specific quality criteria. These include training, validation and testing datasets which will be subject to specific practices listed in Article 10(2). Furthermore, the datasets must be examined '*in view of possible biases'.*[84] However, bias is not defined clearly and this is problematic given that AI provider will not be able to apply appropriate measures under this provision to minimize bias. Although there is EU law which regulates discrimination, none of the provisions specifically target bias in relation to AI and algorithms.[85] These datasets must also be '*relevant, representative, free of errors and complete'.*[86] Such a level of perfection is technically not feasible and might inhibit innovation due to its overly restrictive nature.[87] Within subsequent compromise texts, this has been amended to read '*shall be relevant, representative, and to the best extent possible, free of errors and complete'.*[88] This shows that the regulators are aware that the proposal text is overly restrictive. However, the wording used within the compromise text also introduces uncertainty because there is no industry wide understanding of what level constitutes '*the best extent possible'.*

Finally, this section also introduces a legal basis to process special categories of data as defined under the GDPR for the purposes of bias monitoring, detection and correction in relation to high-risk AI systems.[89] This provision widens the restrictive exceptions currently found within the GDPR for the purposes of processing special categories of personal data.

---

[84] AI Act Art 10(2)(f)
[85] Martin Ebers and others, *The EU Commission's Proposal for an AI Act – A Critical Assessment by Members of the Robotics and AI LAW Society,* The Impact of AI on Law, 2021, 4
[86] AI Act Art 10(3)
[87] Ebers (n85)
[88] Compromise Text (n60) p. 92
[89] AI Act Art 10(5)

There is still the possibility that these provisions are amended since this is still at proposal stage. However, the provisions in relation to data governance would need to be made clearer with specific definitions included in order for this to have a significant effect on sourcing data for training datasets.

3.2.3. EHDS

In May 2022 a proposal was made for a regulation to establish '*domain-specific common European data spaces'* to address issues with electronic health access and sharing within the EU.[90] Due to the uneven implementation of the GDPR[91], barriers are created to the secondary use of health data by researchers, innovators, regulators and policy makers and thus, the aim of the regulation is to '*improve access to and control by natural persons over their personal electronic health data in the context of healthcare…as well as for other purposes that would benefit society such as research, innovation, policy-making…* '[92]

In fact, Article 34 of the Proposal for EHDS provides for access to health data by applicants if they intend to process for specific purposes listed within the article. These include:

- *'development and innovation activities for products or services contributing to public health or social security, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices;*
- *training, testing and evaluating of algorithms, including in medicinal devices, AI systems and digital health applications contributing to public health or social security, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices';*

Although still at proposal stage and with the risk that the provisions may change, it is interesting to note the reference to digital health applications within the text of the current proposal. Although there is no specific definition established, the reference to AI systems and digital health applications acknowledges the fact that such systems need huge datasets to evolve and operate and provides for a way in which such can acquire these datasets in a more regulated manner. In fact,

[90] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, 2022/0140 (COD) ('EHDS')
[91] Article 9(4) of the GDPR allows Member States to maintain or introduce further conditions, including limitations, with regards to the processing of genetic data, biometric data or data concerning health.
[92] EHDS Recital 1

Article 35 goes on to prohibit secondary use of health data in certain instances including when the health data will be made available to third parties not mentioned in the data permit.

Within the context of digital health applications, this proposal hints at the future where further regulations will be enacted to regularize the issues surrounding these applications. Although this is not the main aim of the proposal, it will have a direct effect on regularizing the acquisition of datasets for digital health applications including those which use AI. Since the main aim of the legislation is not to regularize the sourcing and use of training datasets, this legislation does not contribute to regularizing other issues such as bias arising for the datasets and to date, no such legislation tackles the issues surrounding training datasets in AI directly.

Since there is no overarching regulation, this contributes to the further fragmentation of regulation and the indirectly applicable provisions within regulations will affect digital health applications. Although it will tackle the issues related to datasets to a limited extent, this also makes compliance harder since the applications will need to keep up to date with various legislations. It will also make enforcement difficult. Regulating the acquisition of datasets is a good step and a necessary one. However, the type of regulation will also have an impact on the practical effects the regulation has on the market.

3.3. Transparency and Accountability

3.3.1. AI Act

The AI Act is a proposal for a regulation meant to harmonise the use of AI systems in the EU and to classify AI systems according to risk level. Transparency is included in the proposed AI Act to mean '*high-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately'*.[93] This is quite ambiguous and refers to the users of a system which in some instances may not necessarily be the end users. A minimalist interpretation of this suggests that informing users of any potential biases or assumptions taken by the system would be sufficient

[93] AI Act Art 13

since this would allow users to interpret the output.[94] This will need to be clarified further, either in future amendments to the AI Act itself or through guidelines post promulgation since the ambiguity gives the providers leeway to make a distinction between mere disclosure and a more detailed explanation of such disclosure.

The AI Act also requires high-risk AI to include instructions in an appropriate format and in a comprehensible manner. Specifically, the instructions should include contact details of the provider; the characteristics, capabilities and limitation of performance; any changes to the AI systems as pre-determined by the provider at the moment of the initial conformity assessment; any human oversight put in place; and the expected lifetime and maintenance measures.[95] None of the information listed will require the provider to be transparent about the operations of the system, since this information is more aimed towards instructing the users' how to interact with the system.[96]

Accountability is not directly regulated in the AI Act and is only mentioned within the context of high-risk AI systems which are obliged to have a quality management system in place to ensure compliance. Part of this system will include '*an accountability framework setting out the responsibilities of the management and other staff in relation to'* the quality management system.[97]

3.3.2. GDPR

Issues may also arise from the principle of transparency found within the GDPR due to issues with algorithmic explainability. Transparency under the GDPR '*requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used'*.[98] Accountability, on the other hand refers to the controller's responsibility to prove compliance with the principles set out in Article 5(1) which principles were all codified for the purposes of data protection. Furthermore, a right to information about the existence, logic, and envisaged

[94] Madalina Busuioc and others, *Reclaiming Transparency: Contesting the Logics of Secrecy within the AI Act*, European Law Open, Cambridge University Press, 2022 p. 14 <https://www.cambridge.org/core/journals/european-law-open/article/reclaiming-transparency-contesting-the-logics-of-secrecy-within-the-ai-act/01B90DB4D042204EED7C4EEF6EEBE7EA#> last accessed 31st January 2023
[95] AI Act Art 13(2)
[96] Busuioc (n94) p. 14
[97] AI Act Art 17
[98] GDPR Recital 58

consequences of automated decision-making systems as well as the right to object to automated decision-making processes are found in the GDPR.[99] The right to explanation is ambiguous and it is debateable whether this is sufficient explanation to convey meaningful information about AI or automated decision-making systems.[100]

The opaque nature of most AI opposes the transparency required by the GDPR for any AI which processes personal data. It is important to note that the effects of the GDPR are limited to digital health applications which process personal data. In practice, data sets will not be solely composed of personal data and will most often be mixed with non-personal data. In this case, the GDPR will apply to the data set in its entirety. However, any data sets composed of non-personal data solely, will fall outside the scope of the GDPR and will thus be 'unregulated'.[101] Thus, in such situations, regulatory oversight would ensure that decisions may be made on a case-by-case basis depending on the level of risk.

This ties in with the relative freedom allowed by the MDR to manufacturers to categorize the digital health application according to their intentions. A digital health application, may easily classify itself as a well-being application, thus escaping the regulatory compliance required by the MDR. Such applications may go one step further and process '*quasi-health data'*[102] thus managing to avoid the higher level of protection required by the GDPR and undermining the distinction between the categories of personal data.[103]

These unregulated 'loopholes' reduce the regulatory burden on digital health applications but also increase user risks. This also highlights the effects of having indirect general legislation instead of having direct legislation promulgated, following a study of the risks posed to users of these applications.

[99] GDPR Art 13-15, 22
[100] Doshi-Velez (n51) p. 3
[101] Maja Brkan, Gregory Bonnet, *Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: Of Black Boxes, White Bases and Fata Morgana*, Eur. J. Risk Reg. 11(1), 18 p. 3
[102] Within the context of this thesis, this is defined to refer to personal data which may infer health status, but which does not qualify as a special category of personal data.
[103] Marelli (n79) p. 455

3.4. Regulatory Oversight

3.4.1. AI Act

The AI Act has been criticised for its shortcomings on regulatory oversight. There is an obligation on each member state to designate a competent national authority to act as the Market Surveillance Authority.[104] Although the AI Act binds member states to ensure that the authority has sufficient personnel, the fact that a new specialised authority does not need to be created, but one chosen from existing regulators may be assigned, implies that there is likely to be under-specialisation and overburdening.[105] Furthermore, the authority will rely on notifications from the providers of high-risk AI systems to report any incidents within 15 days of becoming aware of such and the authority is in turn bound to report this to the relevant national public authority. The EU Commission will issue guidelines on this process within 12 months of the AI Act coming into force.[106] No mechanism is provided for individuals to report any breaches in a similar manner and this is a significant omission from an accountability perspective, since there will be no independent feedback on any malfunctioning or incidents.[107]

3.4.2. Regulatory Oversight at an EU Level

The co-rapporteurs of the AI Act proposed replacing the AI Board with an independent body established at an EU level. This body would be independent but accountable to the European Parliament and Council. This would mean that there is a specific body, with sufficient specialised knowledge, that is tasked with issuing decisions, guidelines, sandboxes and technical standards thus giving this body the ability to regulate informally.[108]

3.4.3. Regulatory Oversight at a National Level

At the member states' level, based on a study held by the European Commission in 2021, only a few countries are implementing guidelines or rules for AI based product approval. The MDIA in

[104] AI Act Art 59
[105] Madalina Busuioc, *AI Algorithmic Oversight: New Frontiers in Regulation*, Handbook of Regulatory Authorities, Edward Elgar Publishers, 2022, Chapter 31, p. 478
[106] AI Act Art 63-64
[107] Busuioc (n105) p. 478
[108]<https://www.euractiv.com/section/digital/news/leading-meps-push-for-european-office-to-enforce-the-eus-ai-rulebook/> last accessed 24th January 2023

Malta is developing guidelines for registration and certification whilst in Sweden the National Board of Health and Welfare has created conditions for structured and appropriate documentation in health care.[109] These guidelines signify a national interest in regulating AI which bodies and guidelines do not necessarily result from EU legislation but which are not an informal bottom up type of regulation either.

For example, the MDIA was set up to develop the innovative technology sector in Malta[110] and requires the registration of innovative technology arrangements as defined within the legislation.[111] Digital health applications may fall under

> *'software and other architectures…which are used or meant to be used, as a stand-alone or as part of a solution in sectors…which are deemed to be of a risky or critical nature, where their failure or misuse could amongst other things result in loss of life, grave prejudice to the well-being and rights of natural persons…'*[112]

and would thus, fall under the regulatory oversight of the MDIA. This initiative serves to increase regulatory oversight and guidelines through the MDIA and gives regulation a better flexibility in order not to inhibit innovation. However, this is a singular effort taken on a national level and not an EU wide initiative and thus, the benefits from the EU's perspective will be minimal. Furthermore, this regulatory oversight is not specialised and is thus, untrained as to the specific risks arising from AI and in turn the risks to individuals arising from AI in digital health.

[109] Study on Health Data, Digital Health and Artificial Intelligence in Healthcare, EU Commission, July 2021
[110] Chapter 591 of the Laws of Malta
[111] Chapter 592 of the Laws of Malta
[112] Ibid. Schedule 2

4. User Protection or Innovation?

In order to reach a balance between law and innovation we need a regulatory environment which is '*properly geared for risk management and benefit sharing'*.[113] As discussed in Chapter 1, regulating technological innovation may give rise to the challenge of regulatory connection and the pacing problem. These problems appear in the current regulatory environment where AI has been operating under a legislative framework which was generally promulgated prior to the use of AI and which has for the most part not been adapted to the increasing use of AI in various markets including in digital health. Under the EU's Digital Decade, the EU is proposing multiple legislations related to the digital market some of which will have significant effects on digital health.

The structure will follow previous chapters in splitting the issues into four sub-headings: issues related to the classification of AI as a medical device, issues related to health data, issues related to transparency and accountability and issues relating to regulatory oversight. It is difficult to achieve a balanced regulatory environment which ensures protection of users whilst not inhibiting innovation especially within digital health where some users may be vulnerable and require protection. However, these issues relate to basic protections which the legislator already provides for users of more traditional medical devices. Thus, such protections automatically apply to digital health and AI in digital health although some have not been fully adapted to the specific characteristics of such.

This chapter will analyse the effects of the current regulatory environment on users and on innovation within the digital health market whilst keeping in mind the challenges of regulating innovation which have been previously discussed in this thesis.

4.1. Classification of AI as a Medical Device

The issues to be assessed here are two: the first relates to the classification of lifestyle and wellbeing applications separately from medical devices and the second relates to whether the legal provisions regulating AI software as a medical device are sufficiently adapted to the characteristics of AI.

[113] Brownsword (n23)

The regulator uses regulation in relation to classification of medical devices to establish safety standards within the market and to enforce such standards through post-market compliance procedures. This is because medical devices pose a bigger threat to any users.

The applicable legislations are the MDR and the proposed AI Act, where any software which falls within the remit of the MDR or is listed within its annexes will be considered a high-risk AI and subject to more stringent compliance measures.

4.1.1. Lifestyle and Wellbeing Applications

Within the digital health market, lines have become blurred between well-being and lifestyle activities and acts of medicine.[114] The leeway afforded to providers to categorize their application based on the intended use means that there may exist applications which are not marketed as medical devices but which have properties that constitute a medical device had they been marketed that way.[115] These may pose similar or equal risks to users but escape the MDR compliance requirements and in conjunction escape being classified as high-risk AI.

Furthermore, although the guidance document issued under the MDR to define software is promising, to date, no further regulatory steps were taken in relation to AI as a medical software. This also highlights the need for further informal regulatory oversight to be able to solve the pacing problem in the shorter term. The AI Act is a risk-based regulation. However, the risks posed to users arising from applications which are not intended to be used as a medical device, but which have medical properties are not highlighted as risky, and thus, are not subject to appropriate compliance measures.

Within the current market, the EU seems to have indirectly supported innovation within lifestyle or wellbeing applications through its use of a non-risk-based approach in the MDR.[116] This is replicated in the proposed AI Act due to its reliance on the MDR in relation to digital health. This comes at the price of unclear and unmitigated risks for users from the perspective of the medical safety and efficiency of these applications which can have various medical implications.

[114] Paul Quinn, *The EU Commission's Risky Choice for a Non-Risk Based Strategy on Assessment of Medical Devices*, Computer Law & Security Review, 2017, 33 p. 367
[115] Ibid. p. 366
[116] Ibid. p. 362

The regulator in this case has chosen to allow these applications to operate under a non-restrictive legal regime by excluding them from the MDR and the AI Act thus pushing the balance in favour of innovation within these applications as it reduces compliance costs significantly and gives the providers more regulatory freedom and legal certainty.

4.1.2. AI Software as a Medical Device

Another gap in the legislation is related to the AI's self-learning nature. Although the inclusion of software into the definition of a medical device was a promising step forward, AI is different in that it is self-learning and adapts based on the inputs fed to it throughout its use.[117]

The MDR does not establish a post-market surveillance procedure[118] which is adapted to the unpredictability of AI. The proposed AI Act remedies this and includes provisions for data governance and the quality of datasets. The issue with these provisions is that they fail to define the criteria for measuring the quality of the datasets.[119]

In relation to a post-market procedure, the AI Act obliges providers to document a monitoring system which is proportional to the risks of the high-risk AI system which allows for the collection, documentation and analysis of the relevant data collected in order to evaluate continuous compliance.[120] This is a good step from the perspective of user safety but for complex machine learning AI, this will be a difficult compliance obligation.[121] This may introduce some uncertainty into the market including the fact that the compliance costs may vary depending on the complexity of the specific AI systems and may change as systems grow and develop. This may also require multiple technical compliance employees depending on the complexity of the AI system and thus, it may add to the labour cost of the operations.

The regulator established market standards in relation to user protection within the MDR, and thus, manufacturers of AI software as a medical device are aware of existing obligations and face relative certainty as to the applicable rules and the post-market surveillance they will need to comply with.

---

[117] Anastasiya Kiseleva, *AI as a Medical Device: Is it Enough to Ensure Performance Transparency and Accountability?,* European Pharmaceutical Law Review, 2020 4(1) p. 15
[118] MDR Art 86
[119] Ebers (n85)
[120] AI Act Art 61
[121] Ebers (n85)

This does not negatively impact innovation. This stability is further enhanced by the regulator's instrument choice in that the MDR is a regulation and this means that there is relatively uniform application throughout all member states.

Since the MDR was amended to include software as a medical device, AI software which may be classified as a medical device was included into its scope. However, the MDR was not specifically adapted to AI and there are no restrictive provisions for this purpose thus not shifting the stability in any relevant way. From the perspective of the user, the MDR is not well-adapted to AI and does not mitigate risks in relation to the data used to train the AI medical device or the updates and adaptations that the AI will invariably make throughout its lifetime.

The AI Act will change this reality as it introduces some uncertainties and increases the manufacturer's compliance burden with the potential of impacting innovation negatively. The regulator's instrument choice in the AI Act was also a regulation and so there should not be any issues with its uniform application. When new laws are proposed, one cannot foretell how the provisions will be interpreted and adapted in practice and so, we will have to wait to see the effect of this impact.

In conclusion, the current legislative framework defining software as a medical device within the EU is not risk-based. Although the AI Act is risk based, its reliance on the MDR in this instance reduces some of its potential to mitigate risks. On the other hand, this leaves the users at risk from the "unregulated" applications.

4.2. Health Data

The issues to be addressed here relate to sourcing health data for the purpose of training datasets, processing of sensitive personal data by the AI and inferences which may be made from the sensitive personal data.

The regulator felt the need to regulate the processing of health data due to its sensitive nature and the impact any unlawful processing may have on the user. Although robust legislation exists in relation to protecting personal data, there are different legislations or proposed legislations which regulate different issues leading to fragmentation of legislation and complicated compliance. The applicable legislations for the purposes of this thesis are the GDPR, the AI Act and the EHDS.

4.2.1. Sourcing and Processing Health Data

The proposed EHDS has promising provisions in relation to regulating sourcing of training data for AI and the secondary use of personal data for the purposes of innovation, research and AI in medical devices. However, the EHDS' focus is on sourcing the data for lawful purposes through secondary use of electronic health data and thus, no provisions are made related to bias in datasets and forming fair datasets in a transparent manner. These provisions will regularize the acquisition of health data for training datasets, but they add some compliance obligations (for example submission of data access applications)[122] to the providers of AI applications. It remains to be seen how bureaucratic the process to submit this application to the health data access body might be and what the resulting impacts on innovation might be. From the customer's perspective this is a positive step as it regulates EU-wide access to their health data and ensures that good quality data sets are training AI systems which may have an impact on the user's life.

The proposed AI Act also has some data governance provisions in place for high-risk AI which use training datasets and here, there is specific reference to bias in datasets and the quality of datasets. The issue with these provisions is that concepts such as bias are not clearly defined within the context of AI and some of the criteria which the data will be obliged to meet is not practical and technically not very feasible.[123] Should the proposed legislation move forward with these provisions as currently worded, informal regulatory intervention will be needed at an EU level in order to provide clarifying guidelines and reduce inconsistencies and fragmentation. The provisions as currently worded will burden developers with significant legal and compliance costs whilst not fully mitigating risks for users due to their ambiguity and impracticality.

The AI Act makes a promising step when adding a legal basis for the processing of health data for the purposes of bias monitoring, detection, and correction in relation to high-risk AI systems since the GDPR is very restrictive in its exceptions under Article 9.[124] However, it remains to be seen how this will be interpreted, since it doesn't make direct reference to acquiring the data for training high-risk AI systems but only to monitoring, detecting or correcting bias in such systems. Furthermore, this is only for high-risk AI systems, and as was concluded from the previous

[122] EHDS Art 45
[123] Ebers (n85)
[124] AI Act Art 10(5)

sections, this is limited to applications which are considered to be medical devices under the MDR and is thus, limited in scope.

The limited scope of the EHDS and the unclear provisions of the AI Act, hint at a fragmented effort to regularize data sourcing. Both instrument choices for these legislation take the form of regulations thus minimizing issues with uniform application but the provisions will mean future uncertainty and increased compliance costs for developers.

The GDPR prohibits automated decision making and profiling which produce legal or significantly similar effects unless this is necessary for the performance of a contract, authorised under law or based on explicit consent.[125]The EDPB suggests that '*significantly similar effects* include *decisions that affect someone's access to health services'* or a decision which affects the '*circumstances, behaviour or choices of the individual'*.[126]

Presently, developers are operating under the GDPR provisions which are known to them. The prohibition on automated decision making is limited to when a decision is solely taken by automation and when there are significant effects as discussed. This will not apply across the board to all digital health applications but may apply to some which process personal data based on the context of their operations. This provides such developers with relative legal certainty and limits the negative impacts on innovation.

Prior to the development of AI, the regulator's main concern was the processing of health data within a commercial context. This is mirrored in the fact that within the GDPR, the only legislation currently in force, there is limited reference to AI as opposed to multiple reference to processing of health data. With the rise of AI, the proposed EHDS and AI Act, add provisions in relation to sourcing of heath data for training AI and data governance principles. This gives rise to legal fragmentation and additional compliance measures.

[125] GDPR Art 22
[126] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 6th February 2018 p. 21 – 22

4.2.2. Inferences from Health Data

The GDPR defines personal data widely to relate to all data which relates to an identifiable person.[127]It also considers health data as a special category of personal data which requires further protection. The distinction between these categories is clear but for the purposes of digital health and its processing of quasi-health data, this is not sufficient. The focus is primarily on the input side of processing with far less control being given to the data subject over the output's use.[128]

In relation to inferences related to health data which may be made from digital health applications, the only clarifying guidelines which exist were issued by the EDPB in relation to the coronavirus pandemic. Ideally, specific guidelines are issued for lifestyle or well-being applications in order to clarify how quasi-health data should be treated and which provisions should apply to it.

This gives producers a relatively stable environment to operate in with a clear categorization of data. However, this does not help users mitigate their risks in relation to the processing of quasi-health data by digital health applications.

The overall fragmentation of legislation in dealing with the varied issues relating to data, leads to an uncertain future both from an innovation perspective and for users. This is another example of the pacing problem in practice where the existing legislation is not fully adapted to the use of AI and proposed legislation is fragmented and introduced after use within the market has already commenced.

4.3. Transparency and Accountability

The issues to be addressed here relate to transparency and explainability of AI which can be opaque by nature. There are currently no specific regulations which target transparency and accountability in AI in digital health.

This is a clear example of the pacing problem in practice wherein intervening too early with strict provisions may result in harm to innovation and whereas intervening at a later stage and with less strict provisions will mean reduced protection for users and difficulties in regulating.

[127] GDPR Art 4(1)
[128] Marelli (n79) p. 455

The principles of transparency codified within the GDPR were not drafted to regulate AI and this means that they do not translate well to the related issues which arise from AI in digital health. There are specific provisions relating to explainability and information in relation to automated decision making systems within the GDPR. However, there are doubts as to whether this provides enough information to the user.

Furthermore, the principle of purpose limitation as codified serves its purpose of ensuring that people know the purpose for which their data is being processed and that their data is not being used for unknown secondary purposes. However, in relation to AI and its opaque nature, especially in unsupervised learning, it is much more difficult to express the purpose for which such data will be processed clearly and in depth. The AI may identify patterns and provide outputs which are difficult to foresee. As discussed in Chapter 2, in order for these provisions to make more sense for AI, the focus might need to change from purpose limitation to explanation in order to enable users to understand how much influence each type of output has on inputs.

The AI Act defines transparency ambiguously whilst focusing on transparency to enable users to interpret the output.[129] Many authors and policy-makers are equating transparency with explainability in relation to the opacity of AI black boxes.[130] Furthermore, the wording of the current provision allows providers discretion in deciding what '*sufficiently transparent'* and '*appropriate type and degree of transparency'* entails. This gives the providers leeway to decide what features to disclose within an explanation.[131] The inexistence of standards as to what measures should be taken to allow for sufficient interpretation of a system's outputs, will only give the providers even more leeway.[132] The AI Act also includes provisions obliging high-risk AI providers to provide specific instructions to the users but these are aimed at instructing users on how to interact with the system.[133]

The leeway given to providers is balanced by the potential for very high fines[134] but these fines must be implemented into national law, meaning that there might be the possibility of some fragmentation in how they are levied. Transparency will need to be clarified further, and it might

[129] AI Act Art 13
[130] Busuioc (n94) p. 3
[131] Ibid. p. 20
[132] Ibid. p. 21
[133] Ibid. p. 14
[134] AI Act Art 71

be done more efficiently through guidelines which may establish what information and explanation is needed exactly to enable users to understand. The level of information needed may also be adapted to the opacity and complexity of the AI system.

Currently, only AI which processes personal data as part of its service will be bound by the GDPR's provisions relating to explainability and information in relation to automated decision making. This leaves providers quite free to build and continuously improve their product without the need for explainability. Furthermore, the impact of the ambiguous provisions included in the AI Act will only be fully known in the future, once the regulation has been adopted and promulgated.

4.4. Regulatory Oversight

The issue with regulatory oversight in relation to AI is that specialisation is necessary in order to be able to understand the specific characteristics of AI including its self-learning nature and opacity. Sufficiently specialised regulatory oversight may reduce the levels of legal uncertainty created by ambiguous provisions and fragmentation in regulation. Efficient regulatory oversight would be a way to bridge any gaps which arise as time passes and to ensure that regulatory connection is maintained within such a dynamic market.

To this effect, the proposal to establish an independent body at EU level which is responsible for AI would ensure that there is specialised knowledge and oversight which may issue decisions, guidelines and standards. In turn, this would act as a guide for and have a positive impact on the national Market Surveillance Authority[135] which may suffer from under-specialisation or over burdening as discussed in Chapter 3.

This would create more legal certainty which will benefit both innovation and users since it will produce clearer guidelines on the interpretation of provisions in practice and this will make compliance clearer whilst also protecting users better because guidelines result in streamlined interpretation of provisions.

[135] AI Act Art 59

5. How Can the Regulatory Environment be Improved?

5.1. Is this the Ideal Regulatory Environment?

Brownsword and Goodwin established four criteria which regulators have to face when attempting to create an ideal regulatory environment which balances between innovation and regulation as discussed in Chapter 1. These criteria will be used as part of the analysis on whether the existing regulatory environment described in detail in Chapter 3 is ideal to balance between law and technology.

5.1.1. Prudence and Precaution

AI in digital health poses a mix of identifiable and unknown risks to users. Furthermore, the use of AI in digital health is increasing slowly and reaching new areas of the sector. The EU has shown prudence in its risk-based approach to regulating AI. As discussed, the proposed AI Act establishes a hierarchy for risky AI: minimal risk, limited risk, high risk and unacceptable risk. AI systems classified under the first three risk classifications are subject to different compliance measures whilst the latter risk classification prohibits the use of these AI systems.[136] The digital health sector will only be classified as high-risk when such application is also classified as a medical device.

5.1.2. Regulatory Legitimacy

The EU's regulatory toolkit includes two forms of legislation which may be imposed for the topics which fall under its competence: as a regulation or as a directive. A regulation applies automatically and uniformly to all EU countries whilst a directive must be transposed into national law to achieve the objectives set in such directive.[137] All EU proposals for legislation follow a public consultation and a long negotiation process between the different EU entities wherein multiple compromise texts are presented and debated before a final text is agreed on.[138] Health is a competence shared between the EU and national member states and the EU seeks to complement national policies

[136] AI Act p. 12
[137] <https://commission.europa.eu/law/law-making-process/types-eu-law_en#:~:text=There%20are%20two%20main%20types%20of%20EU%20law%20%E2%80%93%20primary%20and%20secondary.> last accessed 08.02.2023
[138] <https://www.europarl.europa.eu/olp/en/interinstitutional-negotiations> last accessed on 27th March 2023

through its health strategy to '*contribute to innovative, efficient and sustainable health systems* and *harness new technologies and practices'*, amongst other things.[139] Therefore the EU has regulatory legitimacy within AI in digital health.

5.1.3. Has the Regulatory Strategy Achieved a Balance?

The EU's digital aim is to create a single market for data flow within the EU with access across all sectors for the benefits of business, research and public administration.[140] The regulatory strategy to achieve this is made up of various regulations and directives, some which have already been enacted and others which are still at proposal level. If we take the perspective of digital health, there are some positive steps forward which will help improve the quality of data for training datasets through easier access[141], for example. But the provisions are fragmented, and compliance costs will be high. Furthermore, enforcement of any penalties established in different legislations may be fragmented and problematic as well.[142]

Has a balance been reached between allowing innovation to flourish and the protection of users? This is debatable since the health sector is one of the most important sectors and deals with generally vulnerable people. The EU regulator has made clear its intention to classify medical devices separately from lifestyle and wellbeing applications. However, whilst the definition of AI as a medical device may be deduced from the MDR, the definition of lifestyle and wellbeing devices automatically amounts to any applications which do not classify as medical devices.

Even if lifestyle and wellbeing applications do not need to be classified as high-risk AI, adding a specific reference to health within Annex 3 of the AI Act might be favourable. One example is health insurance software which uses AI. This is not found in the original wording of the AI Act proposal but can be found within compromise texts under the heading of '*access to and enjoyment of essential private services':*

> *'AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance with the exception of AI systems put into*

[139] Treaty on the Functioning of the European Union Article 168
[140] <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en> last accessed 10.02.2023
[141] This was discussed in Chapter 3 when the EHDS was analysed.
[142] AI Act Art 71 and as discussed in Chapter 4.

service by providers that are micro and small-sized enterprises as defined in the Annex of Commission Recommendation 2003/361/EC for their own use'.[143]

Should this be included within the final text of the AI Act, it would be a step in the right direction. This provision attempts to find a balance and excludes AI systems used by SMEs for their own use. However, there are no implications of a potential inclusion of a separate heading for digital health within Annex III from compromise texts which have been made public to date. This also means that AI systems within digital health which do not classify as a medical device have room to innovate and that the classification between lifestyle and wellbeing applications versus medical devices remains.

In conclusion, presently, the regulatory strategy is limited in two instances. Firstly, it is limited due to the fact that there are still some regulations at proposal stage and thus, there is very little legislation in force which has been adapted to the use of AI in digital health. Secondly, following the overview of the applicable legislation given in Chapter 3, and the analysis undertaken in Chapter 4, fragmentation of legislation is prevalent, and this might harm the intended effects of the regulatory strategy.

5.1.4. Regulatory Connection

It must also be noted that whilst the EU is debating and drafting the various legislations which will be implemented one by one over a number of years, AI will keep developing and thus regulatory connection is important. Technology neutral legislation has better odds at staying connected whilst the technology it attempts to regulate innovates and changes.[144]

In this respect, the EU has made positive steps in enacting technology neutral legislation such as the GDPR. The GDPR is an example of such due to the privacy by design concept and the wide application across all industries; it protects *'personal data regardless of the technology used'*.[145] Such legislation can maintain regulatory connection better as innovation continues to change the use of existing technology and adding new aspects.

[143] Compromise text (n60) p. 199
[144] Brownsword (n28)
[145] <https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en> last accessed 27th March 2023

The AI Act proposal is not fully technology neutral since it lists specific techniques and approaches in Annex 1 and any future technologies developed in relation to AI may escape this scope. Annex 1 has been removed in compromise texts but the specific techniques were then added into the definition of AI thus making it narrower and more specific.[146]

Furthermore, the EDPB and European Data Protection Supervisor ('EDPS') in their opinion have noted that providing an exhaustive list of high-risk AI systems undermines the overall risk-based approach and that the list lacks some significant risks such as the use of AI in determining insurance premiums, for assessing medical treatments or for health research purposes.[147] When compared to the GDPR which applies uniformly across the board for all activities which process personal data, the AI Act, due to its risk-based approach, only imposes additional obligations on high-risk AI systems and prohibits AI which poses unacceptable risks. From an innovation perspective, this might attract AI systems which do not classify as high-risk to the EU but from the user's perspective, there is no uniform protection.

Establishing and maintaining regulatory connection with such a volatile subject is difficult and guidelines and market standards respected across the board might be a solution to help fill in any provisions which are vulnerable to becoming outdated quickly. Furthermore, regulatory connection may also be threatened when there is excessive legal fragmentation. Having varied legislation regulating small sections of operations increases compliance costs significantly for the AI provider and it also reduces the regulator's enforcement power.

5.2. Recommended Improvements

The present regulatory environment constitutes various legislation which may apply in different circumstances and to different AI systems. In summary, within the scope of this thesis, AI in digital health will be regulated by the following regulations:

1. The MDR will classify AI as a medical device and differentiate these from lifestyle and wellbeing applications. This classification will automatically make AI as a medical device a high-risk system under the AI Act.

[146] Compromise text (n60) p. 199
[147] EDPB-EDPS Joint Opinion 5/2021, 18th June 2021 p. 9

2. Sourcing and processing of personal data will be regulated by the GDPR and the AI Act wherein it intersects with the GDPR to add an exception to allow for processing of health data under Article 9 of the GDPR. The AI Act adds further provisions in relation to data governance and the EHDS will also introduce provisions for the secondary use of health data by AI systems.
3. The AI Act also includes some ambiguous provisions in relation to transparency wherein an explanation must be given to users. With regards to regulatory authorities, an existing authority is to be designated in terms of the AI Act and no provisions exist allowing individuals to report breaches directly to the authority.

The pacing problem within AI in digital health is already evident, in that there exists widespread use of AI algorithms and the digital health market has been expanding rapidly, but existing regulation has not been fully adapted and any proposed legislation is still pending. Furthermore, as discussed already, there is high fragmentation, and compliance is difficult to achieve. The focus needs to be on simplifying the compliance process without sacrificing user protection. There are several changes which may be made to the upcoming proposed legislation which would help in creating a more balanced regulatory environment.

5.2.1. User Protection

User protection for any lifestyle or wellbeing digital health applications is limited. Since the MDR does not apply and in turn the AI Act does not apply either, there are very limited provisions which will regulate the use of AI within these applications and there are no binding guidelines or codes of conduct for trustworthy AI.

Given the sensitivity of health data, the vulnerability of people when dealing with their health and wellbeing, the lack of regulation on data governance and sourcing of training datasets for AI and the pace at which this market is growing, the regulation of lifestyle or wellbeing applications or lack thereof should be re-considered. Such applications may not be high-risk AI but there need to be some binding guidelines which ensure the safety of the algorithm in the circumstances in which it operates. These would be an informal manner of regulation which does not hinder innovation by resulting in excessive compliance costs, but which ensures a level of regulatory oversight and encourage the building of seamless market practices. Furthermore, this would give the EU or any

applicable regulators the data necessary to be able to understand when the list of high-risk AI within the AI Act might need to be updated.

For AI as a medical device, compliance costs will be high given that the MDR and the AI Act will both apply. In this instance, a balance is not reached because compliance costs are high due to the classification as a medical device whilst users are not necessarily protected well either. The provisions on transparency and data governance lack detail and unless they are backed up by clarifications or guidelines and industry standards, there will be uncertainty within the market which will limit both innovation and user protection.

Furthermore, clarification is needed into the GDPR's prohibition of automated decision making and profiling when such may affect the circumstances, behaviour or choices of the individual. This may be waived if explicit consent is given. However, it is debatable whether any lifestyle or wellbeing applications which use automated decision making actually acquire explicit consent. This is especially due to the fact that there are no transparency obligations if such AI is not classified as high-risk and thus, individuals will have limited information into the automated decision making, if at all, in such circumstances.

5.2.2. Innovation

To ensure the safe use of AI in digital health, the provisions relating to post-market surveillance need to be clarified. The intrinsic variability of AI means that inputs and outputs need to be monitored in order to be able to assess how the AI system is learning and changing, but the provisions within the AI Act leave it up to the provider to do this in a proportional manner. Guidelines at an EU level which establish specifically what is expected from this monitoring documentation would allow for easier implementation of this compliance obligation and a reduction in uncertainty within the market. In this regard, the proposal to replace the AI Board with an independent EU body would enable guidelines to be implemented as and where necessary at the EU level and help foster innovation through legal certainty.

Clarification also needs to be provided in relation to the responsible authorities and reporting obligations on AI providers. Overlapping responsibilities to report to two different authorities under two different legislations (the AI Act and the GDPR) doubles compliance costs and it is

unclear whether fines can be given under both legislations for the same issue. This will be a red flag for many AI developers.[148]

Further to the clarification and confirmation that a provider cannot be fined separately under two regulations for the same breach, clarification should also be given as to the provisions under the AI Act where an existing authority is to be designated at national level. Ideally, the supervisory authority designated under the AI Act would be in constant communication with the Data Protection Commissioner in order to share resources when investigating the same breaches and reduce any potential for errors as well as the double compliance workload put onto the developers to be in touch with two separate regulators about the same issue.

[148] <https://www.complianceweek.com/risk-management/experts-new-ai-laws-pose-risk-of-overlap-with-data-protection-mandates/32615.article> last accessed 28th March 2023

Conclusion

This thesis aimed to answer the following research question throughout its course:

> *Does the present regulatory environment achieve a balance between innovation in digital health applications which use AI and the protection of users?*

and based on the analysis undertaken throughout this thesis and as explained throughout Chapters 4 and 5, the present regulatory environment does not reach a balance for several reasons. A balance would be reached if the regulatory environment managed to protect users without hindering innovation and in this case, the research has concluded that the current regulatory environment seems to either lean towards innovation to the detriment of users or be unclear and uncertain to the detriment of both innovation and users simultaneously.

Existing legislation which was broadened to include AI in its scope was not fully adapted to the unique characteristics of AI and its self-learning attributes. This results in reduced protection for users although it provides legal certainty for innovation. Furthermore, regulation for lifestyle and wellbeing applications also favoured innovation when they were specifically excluded from the high-risk AI classification, once again reducing protection for users.

The legislation relating to sourcing and processing health data is fragmented and some of the provisions are ambiguous and this negatively impacts both innovation as well as user protection. Moreover, to date, no provisions have been made and no guidelines published in an attempt to regulate the concept of quasi-health data which is processed commonly within digital health applications. Data is one of the most important issues within AI and thus, in order for a balance to be reached, it is imperative that there are clear provisions in relation to data governance so that compliance measures which need to be taken from a provider's perspective are clear. This will benefit both innovation and the users since clearly interpretable provisions will be easier to implement from the provider's perspective and will protect users better.

Finally, provisions in relation to transparency and accountability are a necessity in order to find a balance within the regulatory environment. Such provisions need to be clear enough that compliance with such doesn't hinder innovation and clear enough to actually protect users from the opacity of AI. At the moment, the lack of provisions favour innovation and lack in protecting users.

Bibliography

Articles

Arora A, *Conceptualising AI as a Digital Health Innovation: An Introductory Review, Medical Devices: Evidence and Research* (Auckl 2020)

Aung Y and others, *The Promise of AI: A Review of the Opportunities and Challenges of AI in Healthcare* (British Medical Bulletin 2021)

Bennett Moses L, *How to Think about Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target* (Law, Innovation and Technology 2013)

Brkan M, *Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: Of Black Boxes, White Bases and Fata Morgana* (Eur. J. Risk Reg. 2018)

Busuioc M and others, *Reclaiming Transparency: Contesting the Logics of Secrecy within the AI Act* (European Law Open, Cambridge University Press 2022)

Butenko A, Barouche P, *Regulation for Innovativeness or Regulation of Innovation?* (Law, Innovation and Technology 2015)

Cohen G and others, *The EU AI Strategy: Implications and Challenges for Digital Health* (Lancet Digital Health 2020)

Davenport T, Kalakota R, *The Potential for AI in Healthcare* (Future Healthcare Journal 2019)

Doshi-Velez F and others, *Accountability of AI Under the Law: The Role of Explanation* (arXiv Cornell University 2019)

Ebers M and others, *The EU Commission's Proposal for an AI Act – A Critical Assessment by Members of the Robotics and AI LAW Society* (The Impact of AI on Law, 2021)

Iqbal J, Biller-Andorno N, *The Regulatory Gap in Digital Health and Alternative Pathways to Bridge it* (Health Policy and Technology 2022)

Kiseleva A, *AI as a Medical Device: Is it Enough to Ensure Performance Transparency and Accountability?* (European Pharmaceutical Law Review, 2020)

Marelli L and others, *Fit for purpose? The GDPR and the Governance of European Digital Health* (Policy Studies, 2020)

Matheny M and others, *AI in Health Care, The Hope, The Hype, The Promise, The Peril* (NAM Special Publication Washington DC 2019)

Muehlematter U, Daniore P, Vakinger K, *Approval of AI and machine-learning based medical devices in the USA and Europe (2015-20): A Comparative Analysis* (Lancet Digital Health 2021)

Nelson R, *In Search of Useful Theory of Innovation* (Research Policy 1977)

Smith H, *Clinical AI: Opacity, Accountability, Responsibility and Liability* (AI & Society 2021)

Thomason J, *Big Tech, Big Data and the New World of Digital Health* (Global Health Journal 2021)

Tsang L, *The Impact of AI on Medical Innovation in the EU and US* (Intellectual Property & Technology Law Journal 2017)

Qing Y, *A Legal Framework for Artificial Intelligence Fairness Reporting* (Cambridge Law Journal 2022)

Quinn P, *The EU Commission's Risky Choice for a Non-Risk Based Strategy on Assessment of Medical Devices* (Computer Law & Security Review 2017)

Vayena E, Blasimme A, Cohen G, *Machine Learning in Medicine: Addressing Ethical Challenges* (PLoS Med 2018)

Wiener J, *The Regulation of Technology and the Technology of Regulation* (Technology in Society 2004)

Books

Black J, *What is Regulatory Innovation?*, Regulatory Innovation: a Comparative Analysis (Edward Elgar Publishing 2005)

Brownsword R, *Law, Technology and Society, Re-Imagining the Regulatory Environment* (Routledge 2019) pg 43.

Brownsword R, *Rights, Regulation and the Technological Revolution*, Oxford University Press, 2008, Chapter 6

Brownsword R, Morag Goodwin, *Law and the Technologies of the 21st Century*, Cambridge University Press, 2012, Chapter 3

Busuioc M, *AI Algorithmic Oversight: New Frontiers in Regulation*, Handbook of Regulatory Authorities, Edward Elgar Publishers, 2022, Chapter 31 pg 478

Research Reports

Pelkmans J, *How can EU Legislation Enable and/or Disable Innovation?* European Commission, July 2014

Study on Health Data, Digital Health and Artificial Intelligence in Healthcare, EU Commission, July 2021

EDPB-EDPS Joint Opinion 5/2021

Thesis

Mudler T, *The Role of Law in Protecting Personal Data Generated by Health Apps and Wearables,* (University of Groningen 2022)

Websites

https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe

https://eur-lex.europa.eu/EN/legal-content/summary/supporting-telecommunications-networks-and-digital-service-infrastructures-across-europe.html

https://medium.com/predict/what-is-an-ai-algorithm-aceeab80e7e3

https://hdsr.mitpress.mit.edu/pub/f9kuryi8/release/8

https://data.world/datasets/health

https://commission.europa.eu/law/law-making-process/types-eu-law_en#:~:text=There%20are%20two%20main%20types%20of%20EU%20law%20%E2%80%93%20primary%20and%20secondary

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

https://www.linkedin.com/pulse/definition-digital-health-etymology-plurality-term-paul-sonnier/

https://www.eupatient.eu/policy/Policy/eHealth/#:~:text=Digital%20health%20refers%20to%20healthcare,%2C%20consumer%20health%20informatics%2C%20etc.

https://www.eu-patient.eu/globalassets/policy/ehealth/epf-final-position-paper-on-ehealth_19december2016.pdf

https://med.stanford.edu/news/all-news/2018/11/ai-outperformed-radiologists-in-screening-x-rays-for-certain-diseases.html

https://ai-derm.com/

https://flo.health/faq/accuracy#:~:text=We%20use%20artificial%20intelligence%2C%20an,up%20to%2054.2%25%20more%20accurate.

https://www.euractiv.com/section/digital/news/leading-meps-push-for-european-office-to-enforce-the-eus-ai-rulebook/

https://www.europarl.europa.eu/olp/en/interinstitutional-negotiations

https://www.complianceweek.com/risk-management/experts-new-ai-laws-pose-risk-of-overlap-with-data-protection-mandates/32615.article