AI-powered Medical Devices and the Development Risk Defense Under the Revised Product Liability Directive

Andrea Parziale

Abstract This chapter assesses whether and to what extent the revised Product Liability Directive (RPLD) provide the manufacturers and providers of AI-powered devices for personalized medical solutions with desirable safety incentives. To this end, the chapter outlines relevant aspects of the current safety regulatory framework including the Medical Device Regulation and the AI Act. In complement, the chapter includes an analysis on the role of the RPLD. This analysis focuses on a hypothetical scenario where an autonomous AI-powered medical device that initially seems safe continues to learn and later begins to provide flawed information resulting in patient harm. As such, the discussion centers on the potential benefits and limitations of the new legislation including the exemptions for 'later risk' and 'development risk'. I argue that the RPLD could incentivize manufacturers to react to any emerging risks that become known or knowable. However, the situation is more nuanced for the first victims of unknown risks. This is because the revised product liability regime, while limiting the opportunity for manufacturers to rely on the 'later risk' exemption, lends itself to inconsistent incentives through the 'development risk' defense. This raises the question of whether strict liability should be considered for these kinds of products. The legal systems in which fault-based, product, and strict liability regimes coexist are well placed as 'living laboratories' where one can readily test how these different liability regimes operate.

1 Introduction

In recent years, the integration of AI into medical devices has led to deep transformations in healthcare. While physicians have historically led the assessment, planning, development, delivery, and evaluation of healthcare, human deliberations in

A. Parziale (✉)
LIDER-Lab, DIRPOLIS, Sant'Anna School of Advanced Studies, Pisa, Italy

Health Science Interdisciplinary Center, Sant'Anna School of Advanced Studies, Pisa, Italy
e-mail: andrea.parziale@santannapisa.it

F. Casarosa et al. (eds.), *Enabling and Safeguarding Personalized Medicine*,
Data Science, Machine Intelligence, and Law 7,
https://doi.org/10.1007/978-3-031-99709-9_14

clinical settings are increasingly being assisted by new technologies.[1] In this context, AI-powered medical devices hold the potential to significantly improve patient care, the accuracy of diagnoses, treatment outcomes, and the operational efficiency of healthcare systems worldwide.[2] This is because, among other things, AI can personalize medicine by tailoring diagnostic and therapeutic interventions to the unique genetic, biochemical, physiological, and behavioral features of each individual patient.[3] Emerging data-intensive assays, such as DNA sequencing, proteomics, imaging protocols, and wireless health monitoring devices, are playing a critical role in this personalization process.[4] Big data paradigms are aggregating massive amounts of data from different sources, harmonizing those data, and making them available for analysis to identify patterns that would not and could not otherwise be detected.[5] AI, which includes machine learning, deep learning, neural network constructs, and related techniques, has therefore become essential to both finding relevant patterns in these massive datasets and also for delivering clinically meaningful insights.[6]

Within this changing landscape, AI-powered devices for personalized medical solutions are poised to revolutionize treatment paradigms across various disease conditions.[7] These devices encompass a wide spectrum of innovations, from pharmacogenomic assays that predict medicinal responses based on genetic profiles to wearable biosensors that continuously monitor vital signs and biomarkers in real-time.[8] By harnessing the power of big data analytics and AI, such devices can seamlessly offer insights into disease risk, progression, and response to therapy, enabling clinicians to tailor interventions for optimal outcomes. For example, implantable medical devices equipped with sensors and 'autonomous' AI software can monitor cardiac function in patients with heart failure, predicting exacerbations and adjusting treatment strategies in real-time.[9] Similarly, wearable devices capable of analyzing sweat or blood biomarkers can provide early warning signs of metabolic disorders or infectious diseases, empowering people to take proactive measures to safeguard their health while also assisting in clinical decision-making processes.[10]

However, although incorporating AI into medical devices is showing great potential for personalizing and improving healthcare, it is also raising numerous ethical questions that demand careful consideration.[11] Among these, ensuring patient safety

[1] Amisha et al. (2019), p. 2328.

[2] Briganti and Le Moine (2020).

[3] Bommu and Jeffrey (2024).

[4] Schork (2019), p. 265.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Cherubini and Dinh (2023), p. 404; Donghwan and Enusun (2023), p. 658; Webster (2024).

[9] Gautam et al. (2022).

[10] Shajari et al. (2023), p. 9498; Zhang et al. (2023).

[11] Braun and Harasimiuk (2023), p. 1.

and bodily integrity is of paramount importance. To this end, Regulation (EU) 2017/745 (the Medical Device Regulation, MDR) and Regulation (EU) 2024/1689 (the Artificial Intelligence Act, AI Act) both outline an ex-ante regulatory framework that aims to ensure only safe and effective AI-powered medical devices are placed on the market (or otherwise put into service). Yet 'autonomous' AI systems may lend themselves to behaving in a way that was not anticipated from the outset. For instance, it is entirely possible that, over time, these devices can begin to communicate incorrect information or provide incorrect recommendations. In other words, in its continued learning process, an autonomous AI system may 'learn to make mistakes'. Therefore, it is important that the governing regulatory and liability frameworks incentivize the developers of AI systems to not only react to the emergence of such mistakes in a timely and effective fashion but also to minimize these mistakes from occurring in the first place—at least to the extent possible. Such safety nets are essential to fostering public trust in these crucial innovations.

Against this backdrop, the liability landscape for these and similar technologies is rapidly changing in Europe. Of particular importance will be Directive (EU) 2024/2853 (the revised Product Liability Directive, RPLD). Discussion on this Directive therefore attract the bulk of attention in this chapter. In particular, I assess how well the RPLD might go about providing desirable safety incentives to the developers of AI-powered devices for personalized medicine. As a first step, I provide some background to the regulatory frameworks already in place concerning these kinds of products, highlighting the MDR and the AI Act in particular. Next, I analyze how the RPLD would stand up in a scenario where an autonomous AI-powered medical device at first works safely but, later, starts making mistakes which cause harm to an increasing number of patients. Importantly, the insights established should be highly valuable for informing specific policy recommendations regarding the national implementation of the RPLD. Last, I build on the identified limitations of the RPLD to argue in favor of a strict form of liability for these products, coupled with a call for further research along several specific streams of investigation.

2 The Current Regulatory Framework: The MDR and the AI Act

At the outset, AI-powered devices for personalized medicine are likely to fall under both the MDR and the AI Act. The MDR defines a medical device as any instrument, apparatus, appliance, software, implant, reagent, material, or other article intended by the manufacturer to be used for medical purposes such as diagnosis, prevention, monitoring, treatment, or alleviation of disease.[12] Importantly, if

[12] Medical Devices Regulation (MDR), Regulation (EU) 2017/745 on medical devices, European Parliament and Council (2017) amending Directive 2001/83/EC, Regulation (EC) No 178/2002

software is not qualified as a medical device in itself, it may qualify as an accessory to a medical device when it is integrated into a physical device for the purposes of assisting the device to perform its intended (medical) purpose and therefore the MDR would still apply.[13]

Under the MDR, medical devices must comply with the general safety and performance requirements listed in Annex I to the Regulation. These devices must be designed and manufactured to achieve their intended performance without compromising the safety of patients or users. This involves establishing, implementing, and maintaining a risk management system that is continuously updated throughout the device's lifecycle.[14] Manufacturers are also required to document a risk management plan, identify and analyze foreseeable hazards, and implement control measures to eliminate or reduce risks.[15] Additionally, manufacturers must ensure that any residual risks are communicated to users and are acceptable when weighed against the benefits of the device.[16]

The MDR also imposes specific requirements for software, including ensuring repeatability, reliability, and performance in line with the software's intended use.[17] The software must be developed according to state-of-the-art principles that consider risk management, verification, and validation. Moreover, if the software is intended for use with mobile computing platforms, it must account for the unique features of mobile environments.

Classifying the device under Annex VIII of the MDR is crucial for determining the level of regulatory scrutiny each product will undergo and the applicable post-marketing obligations. Rule 11 of the MDR classifies software intended for decision-making in diagnosis or therapy as Class IIa, except when such decisions may cause: (i) a serious deterioration of the health status of a person or a surgical intervention (in which case, it falls into Class IIb); or (ii) death or an irreversible deterioration of the health status of a person (in which case it belongs to Class III). Software intended to monitor physiological processes falls into Class IIa, unless it is intended for monitoring vital physiological parameters, where variations in these signs could result in immediate danger to the patient (in which case, it falls into Class IIb). Any other software is allocated to Class I. Importantly, software that drives or influences a device falls under the same class as the device itself.

While there are numerous classification criteria in Annex VIII to be applied on a case-by-case basis, the MDCG 2019-11 Guidance document[18] to the MDR suggests that AI-powered devices for personalized medicine are likely to fall into the

---

and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, Official Journal of the European Union, L 117/1. Article 2(1).

[13] MDR, Article 2(2).

[14] MDR, Annex I, Section 3.

[15] Ibid.

[16] MDR, Annex I, Section 23.1.

[17] MDR, Annex I, Section 17.

[18] MDCG (2019), Annex 3.

medium-to-high risk categories. This means that the products will likely need to be certified by a Notified Body. In addition, the device will have to comply with the obligations pertaining to Clinical Evaluation Reports, Post-market Surveillance Plans, Periodic Safety Update Reports, Post-market Clinical Follow-up Plans, Post-market Clinical Follow-up Reports, and Summaries of Safety and Clinical Performance. Clinical Evaluation Reports document clinical evaluations of the device, its results, and the clinical evidence derived from it.[19] Clinical Evaluation Reports for Class IIb and III devices, must be updated annually. The Post-market Surveillance Plan is part of the post-market surveillance system.[20] It proves compliance with the post-marketing obligations set out in Article 83 of the MDR, including the criteria and processes for the risk-benefit assessments of the device and for collecting and analyzing data, addressing complaints, and communicating data to regulatory bodies.[21] The Periodic Safety Update Reports summarize the results and conclusions of the analyses of the post-market surveillance data gathered through the Post-market Surveillance Plan, along with a description of any preventive and corrective actions taken.[22] Again, the Periodic Safety Update Reports for Class IIb and III devices must be updated annually. The Post-market Clinical Follow-up Plan aims to confirm device safety and performance, identify unknown side-effects, analyze emerging risks, maintain an acceptable risk-benefit ratio, and detect misuse.[23] The accompanying Post-market Clinical Follow-up Report documents the outcomes of the Post-market Clinical Follow-up Plan and forms part of the Clinical Evaluation Report and its technical documentation.[24] Finally, the Summary of Safety and Clinical Performance outlines evidence for the safety, performance, and clinical benefits of Class III and implantable devices, and forms part of the technical documentation.[25]

Turning now to the AI Act, an AI system is defined as a machine-based system designed to operate autonomously, capable of adaptiveness after deployment, and capable of generating outputs (such as predictions, recommendations, or decisions) that influence physical or virtual environments.[26] AI-powered devices for personalized medicine likely qualify as high-risk AI systems. This is because the AI in a device is typically considered to be one of the product's safety components, which is covered by the EU harmonization legislation listed in Annex I. This means the

[19] MDR, Article 61(12).

[20] MDR, Article 84.

[21] MDR, Annex III.

[22] MDR, Article 86.

[23] MDR, Annex XIV.

[24] Ibid.

[25] MDR, Article 32.

[26] Artificial Intelligence Act (AI Act) Regulation (EU) 2024/1689 European Parliament and Council (2024) laying down harmonized rules on artificial intelligence', Official Journal of the European Union, L 132/1. Article 3(1).

product or system must undergo a third-party conformity assessment before being placed on the market or deployed into service.[27]

Thus, an AI-powered medical device is likely to meet the qualification criteria for falling under both the MDR and the AI Act and that means that, again, the device will need to be certified by a Notified Body. The manufacturer or provider would also need to consider the product's "intended purpose as well as the generally acknowledged state of the art on AI".[28] Additionally, if a product includes an AI system that falls under both the AI Act and a piece of harmonized EU law, such as the MDR, "providers shall have a choice of integrating, as appropriate, the necessary testing and reporting processes, information and documentation they provide with regard to their product into documentation and procedures that already exist and are required under the Union harmonisation legislation listed in Section A of Annex I".[29]

In the context of high-risk AI systems, a comprehensive risk management system must be established, implemented, documented, and maintained.[30] This system should be a continuous and iterative process, planned and executed throughout the entire lifecycle of the AI system. This includes identifying and analyzing known and reasonably foreseeable risks that the AI system may pose to health, safety, or fundamental rights when used as intended. Additionally, the system must estimate and evaluate risks that could emerge from both intended use and reasonably foreseeable misuse. The risk management process must also include a process of evaluating risks based on any data gathered from post-market monitoring activities or as part of adopting targeted measures to address identified risks. The focus is on mitigating or eliminating risks that can be managed through the design, development, or provision of adequate technical information. High-risk AI systems must undergo testing to identify the most appropriate risk management measures, ensuring consistent performance and compliance with regulatory requirements. This testing may include real-world conditions and should occur at various stages of development, but always before the AI system is placed on the market. Moreover, the testing needs to be conducted against predefined metrics and probabilistic thresholds appropriate to the intended purpose of the AI system.

In addition, a single set of technical documentation must be prepared that demonstrates compliance with both the AI Act and the other relevant EU harmonized legislation.[31] Also, the design and development of high-risk AI systems must ensure sufficient transparency to allow deployers to interpret and use the system's outputs appropriately.[32] Furthermore, providers must have a quality management system to

[27] AI Act, Article 6(1).

[28] AI Act, Article 8(1) AI Act.

[29] AI Act, Article 8(2).

[30] AI Act, Article 9.

[31] AI Act, Article 11.

[32] AI Act, Article 13.

ensure that the AI system complies with the AI Act.[33] This includes examination, testing, and validation procedures to be carried out before, during, and after the development of the high-risk AI system, a risk management system, a post-market monitoring system, and a reporting system for serious incidents. Finally, if a high-risk AI system presents a risk, providers must investigate the causes, collaborate with deployers, inform market surveillance authorities, and take corrective actions.[34]

3 The Role of the Revised PLD

With the current regulatory framework sketched out, we will turn to the potential benefits and likely limitations presented by the RPLD. The RPLD clarifies that, for all the intents and purposes of the legislation, software is a product,[35] which may well include (autonomous) AI systems. To recover damages under the RPLD, the claimant must prove "the defectiveness of the product, the damage suffered and the causal link between that defectiveness and that damage".[36] A product is defective if "it does not provide the safety that a person is entitled to expect or that is required under Union or national law" considering all circumstances.[37]

These circumstances include, but are not limited to, the presentation and characteristics of the product, including its design and instructions; the reasonably foreseeable use of the product; the ability of the product to continue to learn or acquire new features after it is placed on the market or put into service; and the specific needs of the group of users for whose use the product is intended. The non-exhaustive list of relevant circumstances to be considered when attempting to determine whether a product is defective is longer than the existing Product Liability Directive,[38] and some additions seem particularly relevant to AI-powered products. However, others are ambiguous in terms of how they might shape safety expectations. For instance, it is not immediately clear whether the ability of the product to continue to learn (which is a clear reference to AI-powered products) should increase or decrease safety expectations.[39] After all, it is quite foreseeable that an autonomous AI system, by continuing to learn, may end up making mistakes, which would

[33] AI Act, Article 17.

[34] AI Act, Article 20.

[35] Revised Product Liability Directive (RPLD), Directive (EU) 2024/2853, European Parliament and Council on liability for defective products and repealing Council Directive 85/374/EEC, Official Journal of the European Union, L 2024/2853. Article 4(1) and Recitals 6 and 13.

[36] RPLD, Article 10(1).

[37] RPLD, Article 7(1).

[38] Product Liability Directive (PLD), Directive (EU) 2024/2853, European Parliament and Council (2024) on liability for defective products, Official Journal of the European Union, L 289/12.

[39] De Bruyne et al. (2023).

decrease safety expectations and make it harder for claimants to prove a product's defectiveness.[40] However, Recital 32 of the RPLD explicitly states that…

> …the effect on a product's safety of its ability to learn or acquire new features after it is placed on the market or put into service should also be taken into account to reflect the legitimate expectation that a product's software and underlying algorithms are designed in such a way as to prevent hazardous product behaviour.

Thus, the intention of European lawmakers seems to be that a product's ability to self-learn should be seen as something that increases safety expectations. A second issue pertains to the role of the product presentation and its instructions, particularly when the product's instructions warn that it may start giving incorrect information.[41] However, this may be an attempt by the manufacturer to shift liability risks to the users, including healthcare professionals.[42] Yet, it is hard to argue that such a vague warning could effectively shape anyone's safety expectations. Similar to the generic warnings in a medicine's leaflet that "side-effects may occur", it is unlikely that the manufacturer could dodge liability on the basis of such precautions. Since the role of AI-powered devices for personalized medicine needs to be considered, the "special needs of the users" may also have some part to play in increasing safety expectations for a product, as individual patients can reasonably expect that such a device will deliver outputs that are both safe and effective, particularly to themselves.

Finally, Article 10 of the RPLD provides several facilitations to the claimant to prove a product's defectiveness, such as if the manufacturer fails to disclose relevant evidence requested by the claimant or if the claimant demonstrates that the product fails to comply with mandatory safety requirements in the EU or under any domestic law. A causal link between damage and defect is also presumed if such a link has already been established through precedent,[43] or if the claimant faces excessive difficulties in proving such a link, especially if those difficulties are technical or scientific.[44]

Importantly, the manufacturer has the right to rebut any of these presumptions.[45] And even once the claimant succeeds in demonstrating the constituting elements of product liability, the manufacturer can still avoid liability by invoking one of the exemptions listed in Article 11. In the case of autonomous AI-powered products, the most relevant exemptions are when "it is probable that the defectiveness that caused the damage did not exist at the time the product was placed on the market, put into service or, in the case of a distributor, made available on the market, or that that defectiveness came into being after that moment",[46] known as the 'later defect' exemption. Notably, this exemption cannot be applied if the defect is

[40] Ibid.

[41] Duffourc and Gerke (2023), p. 77.

[42] Ibid.

[43] RPLD, Article 10(3).

[44] RPLD, Article 10(4).

[45] RPLD, Article 10(5).

[46] RPLD, Article 11(1)(c).

software-related.[47] Thus, if an autonomous AI system becomes defective due to its ability to continue to learn, the manufacturer will not be able to invoke this exemption.[48]

Another exemption manufacturers can use occurs when "the objective state of scientific and technical knowledge at the time the product was placed on the market or put into service or during the period in which the product was within the manufacturer's control was not such that the defectiveness could be discovered".[49] This is known as the 'development risk' or the 'unknown risk' exemption.[50] This defense can only be use if the product was always defective from the start, but the defect could not be discovered in light of "the most advanced level of objective knowledge accessible and not to the actual knowledge of the economic operator".[51] A manufacturer may, therefore, try to invoke this exemption in lieu of the 'later defect' by arguing that, while the product defectiveness manifested itself at a later stage, the defect must be due to an issue in the original programming of the AI system, which could, unfortunately, not be discovered at the time. This line of reasoning, however, would not be convincing. This is because it conflates the two concepts of (a) there being a defect and (b) the cause of that defect. Indeed, a product is deemed to be defective if it fails to meet the relevant safety expectations. This is irrespective of what the cause of the defect might be. Thus, in the scenario under consideration, the development risk defense would not apply. Further, the manufacturer would not be able to rely on the later defect exemption by virtue of Article 11(2)(b). Thus, the later defect risk seems more likely (not) to apply to autonomous AI-powered medical devices than the development risk defense. To successfully use the development risk defense, the manufacturer would need to demonstrate that the AI system was actually defective from the start. This may provide incentives that, to say the least, would be quite odd in light of the safety requirements mandated by the MDR and the AI Act.

Let us now assume the case of an autonomous AI-powered medical device intended to deliver personalized medical solutions that at first seems to be working as planned but later, by continuing to learn, starts providing flawed information and recommendations that cause harm to patients. Once this emerging risk becomes known or knowable to the manufacturer or provider, and the latter fail to take timely action, establishing liability under the RPLD does not seem to be an insurmountable task. The dense network of requirements laid down in the MDR and AI Act seem particularly helpful to claimants willing to demonstrate product defects or faults, and the disclosure obligations and causal presumptions seem to have the potential to ease the evidentiary burden on the claimants. In particular, the potential interpretive

[47] RPLD, Article 11(2)(b).

[48] Ibid.

[49] RPLD, Article 11(1)(e).

[50] De Bruyne et al. (2023).

[51] RPLD, Recital 52.

ambiguities of some of the circumstances relevant to determine product defectiveness can be solved quite easily in favor of the claimant.

That said, the situation is more nuanced when it comes to the very first victims of an autonomous AI-powered medical device, which unexpectedly starts delivering harmful output (or failure to produce output). In this case, the RPLD does offer some room for recovery to the claimant in such cases, since the later defect defense does not apply if this is due to software. However, the persisting operation of the development risk defense may provide an odd incentive to the manufacturer. The manufacturer can avoid liability by demonstrating that the AI system was defective from the outset, but such a defect could not be discovered. This does not seem to fully incentivize the manufacturer to make sure that the AI-powered product is safe from the outset. Rather, it seems to convey an incentive not to study and test the product in a way that expands the objective state of the art, in order to have room to potentially rely on the development risk defense itself.

This raises the question of whether the Member States should consider derogating from the development risk defense, as allowed by Article 18 of the RPLD. Article 18(2) and (3) impose some conditions on Member States considering amending their legal systems to this end. These conditions include that this must be limited to specific categories of products, in the public interest, and proportionate to achieve the public interest. Since Member States have quite some leeway when it comes to defining what is in the public interest, these conditions do not seem to impose an insurmountable obstacle to exclude autonomous AI-powered medical devices from the development risk defense.

4 Conclusions and Avenues for Further Research: The Role of Strict Liability

Excluding the later defect exemption for software would move the product liability regime closer to a strict liability model. Derogating from the development risk defense, which would already be quite difficult for manufacturers in this domain to use, would also be a decisive step in this same direction. Member States could also consider introducing a form of strict liability for such products on a basis other than defectiveness. Recital 11 clarifies that the RPLD does not preclude the Member States from adopting contractual or extracontractual liability regimes (including strict liability ones) with a basis different from product defectiveness. The strict liability regime for abnormally dangerous activities, along the lines of Article 5:101 of the Principles of European Tort Law[52] offers a useful reference model. The article states:

> Abnormally dangerous activities: (1) A person who carries on an abnormally dangerous activity is strictly liable for damage characteristic to the risk presented by the activity and resulting from it. (2) An activity is abnormally dangerous if (a) it creates a foreseeable and

[52] Busnelli et al. (2005).

> highly significant risk of damage even when all due care is exercised in its management and (b) it is not a matter of common usage. (3) A risk of damage may be significant having regard to the seriousness or the likelihood of the damage. (4) This Article does not apply to an activity which is specifically subjected to strict liability by any other provision of these Principles or any other national law or international convention.

It has been argued in the law and economics literature that this may be particularly justified in the case of developers.[53] Since these "exert a considerable influence on accident risk and often also have 'deep pockets' […], they should be subject to strict liability. Such a regime would generate incentives for both optimal care and optimal activity levels as well as facilitating the effective spreading of risk".[54] Against this backdrop, further empirically-oriented research of a comparative nature could help shed light on the actual socio-economic impact of different kinds of civil liability in this domain, offering insights to inform policy decision-making.

To this end, the European legal framework where fault-based liability, product liability, and outright strict liability regimes coexist seem particularly well placed to be 'living laboratories' where we could test the actual potential and limitations of each kind of liability regime with respect to AI-powered medical devices. As such, it would be highly worthwhile comparing the EU framework to other legal systems where fault-based claims and product liability exhaust claimants' avenues for recovering damages. For instance, consider the Italian legal system where a form of strict liability for dangerous activities is enshrined in Article 2050 of the Civil Code.[55] Under this law, the performer of a dangerous activity is liable unless they can prove they took all adequate measures to prevent the damage. This code could easily be applied to high-risk medical devices and AI systems, offering an ideal testbed for further legal and policy research of a comparative nature.

Acknowledgements This research was financially supported by the "Biorobotics Research and Innovation Engineering Facilities" "IR0000036" – CUP J13C22000400007 (BRIEF) project.

Disclosure of Interests The authors have no competing interests to declare that are relevant to the content of this article.

References

Amisha MP, Pathania M, Rathaur VK (2019) Overview of artificial intelligence in medicine. J Family Med Prim Care 8(7):2328–2331. https://doi.org/10.4103/jfmpc.jfmpc_440_19

Bommu R, Jeffrey B (2024) Revolutionizing healthcare with AI: advancements in medical device software. Int J Adv Eng Technol Innov 1(3)

Braun T, Harasimiuk DE (2023) AI deployment in medical devices-ethical and regulatory reflections, beyond data protection and bias – EU perspective. In: 2023 IEEE Conference on Computational Intelligence in Bioinformatics and Computational Biology (CIBCB), Eindhoven, Netherlands, pp 1–6. https://doi.org/10.1109/CIBCB56990.2023.10264892

[53] Li et al. (2022), pp. 618–634.

[54] Ibid.

[55] See Comporti (2009), p. 149; Cendon (2008), p. 801; Rossetti (2011), p. 693.

Briganti G, Le Moine O (2020) Artificial intelligence in medicine: today and tomorrow. Front Med 70(5). https://doi.org/10.3389/fmed.2020.00027
Busnelli FD et al (2005) Principles of European tort law. Text and commentary. Springer, Vienna
Cendon P (ed) (2008) Commentario al Codice Civile. Artt. 2043-2053. Fatti illeciti. Giuffrè, Milano, p 801
Cherubini A, Dinh NN (2023) A review of the technology, training, and assessment methods for the first real-time AI-enhanced medical device for endoscopy. Bioengineering 10(4):404. https://doi.org/10.3390/bioengineering10040404
Comporti M (2009) Fatti illeciti: le responsabilità oggettive. Artt. 2049-2053. In: Schlesinger F, Busnelli FD (eds) Il Codice Civile. Commentario. Giuffrè, Milano, pp 149 ff
De Bruyne J, Dheu O, Ducuing C (2023) The European Commission's approach to extra-contractual liability and AI –an evaluation of the AI liability directive and the revised product liability directive. Comput Law Secur Rev 105894. https://doi.org/10.1016/j.clsr.2023.105894
Donghwan K, Eunsun K (2023) AI-powered medical devices for practical clinicians including the diagnosis of colorectal polyps. J Korean Med Assoc 66(11):658–666
Duffourc M, Gerke S (2023) The proposed EU Directives for AI liability leave worrying gaps likely to impact medical AI. NPJ Digit Med 6:77. https://doi.org/10.1038/s41746-023-00823-w
European Parliament (2024) Legislative resolution of 12 March 2024 on the proposal for a directive of the European Parliament and of the Council on liability for defective products (COM(2022)0495 – C9-0322/2022 – 2022/0302(COD))
Gautam N et al (2022) Artificial intelligence, wearables and remote monitoring for heart failure: current and future applications. Diagnostics 12(12):2964. https://doi.org/10.3390/diagnostics12122964
Li S, Faure MG, Havu K (2022) Liability rules for AI-Related harm: law and economics lessons for a European approach. Eur J Risk Regul 13(4):618–634. https://doi.org/10.1017/err.2022.26
MDCG (2019) Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, MDCG 11-2019
Rossetti M (2011) Art. 2050. Responsabilità per esercizio di attività pericolose. In: Carnevali U (ed) Dei fatti illeciti. Utet, pp 198 ff
Schork NJ (2019) Artificial intelligence and personalized medicine. Cancer Treat Res 178:265–283. https://doi.org/10.1007/978-3-030-16391-4_11
Shajari S, Kuruvinashetti K, Komeili A, Sundararaj U (2023) The emergence of AI-Based wearable sensors for digital health technology: a review. Sensors 23(23):9498. https://doi.org/10.3390/s23239498
Webster P (2024) How AI-powered handheld devices are boosting disease diagnostics - from cancer to dermatology. Nat Med News, 12 March 2024
Zhang Y, Hu Y, Jiang N, Yetisen AK (2023) Wearable artificial intelligence biosensor networks. Biosens Bioelectron 219. https://doi.org/10.1016/j.bios.2022.114825