European Journal of Law and Technology, Vol. 15 No. 3 (2024)

EJLT European Journal of Law and Technology

The Renewed EU Legal Framework for Medical AI

Sofia Palmieri[*]

Abstract:

The use of artificial intelligence (AI), along with its possible risks and promised benefits, has attracted much attention, filling pages of scientific literature. At the same time, the legal literature has been busy outlining the legal framework applicable to AI systems used in medicine: mainly the Medical Device Regulation (MDR) and the AI Act. The literature has already pointed out the gaps in this legal framework, emphasising its limited significance for AI systems classified as 'minimal risk' under the AI Act. This paper builds upon this literature and overviews the broader product safety framework applicable to medical AI. In this light, while the MDR remains the main co-regulator of medical AI, numerous other regulations interact with the AI Act while regulating medical AI. Starting from the shortcomings of the relationship between MDR and the AI Act, this paper maps the product safety framework applicable to medical AI. Referring in particular to other regulations within the EU New Legislative Framework, it offers the safety framework relevant for AI systems classified for different reasons as minimal risk under the AI Act.

Keywords: AI Act; medical AI; AI system product safety; EU New Legislative Framework; AI-based medical devices.

[*] PhD candidate in Health Law, Metamedica Unit, Department of Public Health and Primary Care, Faculty of Medicine and Health Science, Ghent University, Belgium.

1. Introduction

The use of artificial intelligence (AI) in healthcare, and its perks and perils, have been in the spotlight since the White Paper on Artificial Intelligence was published in 2020.[1] While drafting the document, the European Union (EU) Commission was acutely aware of medical AI, mentioning healthcare solutions in its opening statement. The European Parliament has given it the same attention, publishing in 2022 a study specific to Artificial Intelligence in Healthcare ('the Study').[2] The Study centres on the risks of AI in medicine and possible strategies to curb safety concerns. The academic literature has followed suit, with numerous publications engaging with the risks of medical AI.[3] At the same time, legal academic literature produced a considerable number of papers discussing the applicable legal framework to medical AI. In particular, Schneeberger et al.[4] described the general framework for medical AI, considering various pieces of legislation, such as fundamental rights treaties, the Medical Device Regulation (MDR)[5] and the General Data Protection Regulation (GDPR).[6] Nonetheless, the four years since Schneeberger et al.'s paper was published have seen considerable change in the EU *acquis* regarding AI regulation, notably the drafting of the long-awaited AI Regulation (AI Act).[7] The AI Act proposal, introduced by the European Commission in April 2021, outlined a regulatory framework for AI, and after extensive debates, revisions and approval by the European Parliament and Council, it evolved into the AI Act, a legally binding regulation. This process involved refining the initial draft to address concerns and ensure a balance between innovation, security and human rights. Some authors gave an overview of the main legislations applicable to medical AI,[8] mainly focusing on

[1] European Commission, 'White Paper on AI − A European Approach to Excellence and Trust' (2020).

[2] European Parliament, 'Artificial Intelligence in Healthcare: Applications, Risks, and Ethical and Societal Impacts' (2022).

[3] Maximilian Kiener, 'Artificial Intelligence in Medicine and the Disclosure of Risks' (2021) 36 *AI & Society* 705; Peter Lee, Sebastien Bubeck and Joseph Petro, 'Benefits, Limits, and Risks of GPT-4 as an AI Chatbot for Medicine' (2023) 388 *New England Journal of Medicine* 1233; Ezio Di Nucci, 'Should We Be Afraid of Medical AI?' (2019) 45 *Journal of Medical Ethics* 556.

[4] David Schneeberger, Karl Stöger and Andreas Holzinger, 'The European Legal Framework for Medical AI', *Machine Learning and Knowledge Extraction* (Springer 2020).

[5] 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.

[6] 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) (Text with EEA relevance).

[7] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

[8] Emilia Niemiec, 'Will the EU Medical Device Regulation Help to Improve the Safety and Performance of Medical AI Devices?' (2022) 8 *Digital Health* 205520762210890; Nicholas Terry,

the AI Act and its intertwining with the Medical Device Regulation (MDR).[9] This paper builds upon this literature and offers an overview of the broader safety framework applicable to medical AI.

More specifically, the paper dives into the legislative framework for medical AI intended as a product. In this light, while the MDR remains the main co-regulator of medical AI, numerous other regulations have come into existence or have been reformed and interact with the AI Act while regulating medical AI. As such, the General Product Safety Regulation (GPSR)[10] and cybersecurity-related legislation play an important role in ensuring medical AI safety. Starting from the shortcomings of the relationship between MDR and the AI Act already highlighted in the literature, this paper focuses on the product safety framework applicable to medical AI. In particular, it refers to other regulations within the European Union (EU) New Legislative Framework (NLF), offering the safety framework relevant for AI systems classified for different reasons as minimal risk under the AI Act.

Section 1.1 defines medical AI and sets the boundaries for our discussion. Next, Section 1.2 briefly recalls the EU primary and secondary law as applicable to medical AI. Section 1.3 recapitulates the AI Act safety framework and its risk classification. Based on this, the paper highlights the relevant point of contact between the AI Act and MDR's risk classifications. Based on this exercise, Section 2 reframes the issue concerning medical AI systems falling outside the AI Act high-risk class. The analysis continues in Sections 3 and with an examination of the relevant regulations contributing to the medical AI product safety framework.

1.1 What do we Mean by 'Medical AI'?

To date, AI has progressively been introduced into virtually all areas of medicine, from primary care to rare diseases, emergency medicine, biomedical research, and public

'Of Regulating Healthcare AI and Robots' (2019) 21 *Yale Journal of Law and Technology* 133; R Beckers, Z Kwade and F Zanca, 'The EU Medical Device Regulation: Implications for Artificial Intelligence-Based Medical Device Software in Medical Physics' (2021) 83 *Physica Medica* 1; Anastasiya Kiseleva, 'AI as a Medical Device: Is It Enough to Ensure Performance Transparency and Accountability in Healthcare?' <https://papers.ssrn.com/abstract=3504829> accessed 17 June 2021; M Quaranta and I Angela, 'Obligation for AI Systems in Healthcare: Prepare for Trouble and Make It Double?', *AI Compliance Mechanism (WAICOM 2022)* (2022).

[9] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance); Sofia Palmieri and Tom Goffin, 'A Blanket That Leaves the Feet Cold: Exploring the AI Act Safety Framework for Medical AI' (2023) 30 *European Journal of Health Law* 406; Sofia Palmieri, Paulien Walraet and Tom Goffin, 'Inevitable Influences: AI-Based Medical Devices at the Intersection of Medical Devices Regulation and the Proposal for AI Regulation' (2021) 28 *European Journal of Health Law* 1; Mathias Karlsen Hauglid and Tobias Mahler, 'Doctor Chatbot: The EU's Regulatory Prescription for Generative Medical AI' (2023) 1 *Oslo Law Review* 1.

[10] Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (Text with EEA relevance).

health. Many management aspects related to health administration (e.g. increased efficiency, quality control, fraud reduction) and policy are also expected to benefit from new AI-mediated tools. The medical AI panorama seems to stretch as far as your eyes can go. Therefore, as a preliminary note to this paper, it seems appropriate to answer a fundamental question: What do we mean by medical AI?

While there is still no consensus on what precisely medical AI is, narrow definitions may limit the scope of medical AI to clinical AI solutions. However, in this paper, medical AI will be defined as an AI system operating in the complex and broad environment described by the term 'healthcare', extending the reach of medical AI systems beyond that of medical practice. In further defining medical AI, I follow the lead of the European Parliament,[11] which defines medical AI as a 'type of AI which is focused on specific applications in medicine or healthcare'.[12] While this might look like a rather undescriptive definition, the Study further identifies four main areas of use that better describe medical AI's definition.[13] Adopting the approach therein elaborated in this paper, medical AI is intended to embrace AI solutions for clinical practice, biomedical research, public health and health administration.[14]

1.2 Fundamental Rights

The starting point for this analysis is the impact of medical AI on fundamental rights and patients' rights. As the literature has already extensively discussed, errors inherent in the design of medical AI can result in serious safety risks for the patient.[15] These errors in AI design can lead to various adverse outcomes. Biases in the training data of medical AI systems can lead to safety risks that might infringe patient and fundamental rights. As an example of the risks related to data biases, AI systems might lead to missed diagnoses (false negatives) or suggest that the patient be submitted to unnecessary or inadequate treatment (false positives or inaccurate diagnosis).[16] More generally, biases in training data can lead to the violation of rights such as the right to non-discrimination in access to healthcare services when AI systems are used to schedule doctor`s appointments.[17] Additionally, medical AI often relies on large datasets containing sensitive personal health information. Biases in these datasets can compromise individuals' right to privacy if their data is misused or if they are unfairly targeted based on characteristics such as race, ethnicity or socioeconomic status.[18] The integration of AI in healthcare also introduces concerns regarding the right to information and informed consent. However, these infringements stem from the

[11] European Parliament (n 2).

[12] ibid.

[13] Therein referred to as 'practices'.

[14] European Parliament (n 2).

[15] Robert Challen and others, 'Artificial Intelligence, Bias and Clinical Safety' (2019) 28 *BMJ Quality & Safety* 231; Eric Sutherland, 'Artificial Intelligence in Health: Big Opportunities, Big Risks' (*oecd.ai*, 1 August 2023).

[16] Yoshimasa Horie and others, 'Diagnostic Outcomes of Esophageal Cancer by Artificial Intelligence Using Convolutional Neural Networks*'* (2019) 89 *Gastrointestinal Endoscopy*.

[17] 'Ethics and Governance of Artificial Intelligence for Health: WHO Guidance' (World Health Organization 2021).

[18] European Parliament (n 2).

utilisation of AI itself rather than inherent flaws in its functionality or safety. Instead, they pivot on the ethical considerations surrounding the judicious implementation of AI within the doctor−patient relationship. Consequently, these issues fall beyond the purview of this paper. I refer the reader to the literature in note 19 to further explore this topic.[19]

Against this background, Schneeberger et al. started their analysis by emphasising the importance of fundamental human rights as an essential legal guideline for regulating medical AI. The European Charter of Fundamental Rights (CFR) is the primary source of this framework. It is entirely relevant to the use of medical AI, as the provision of medical services is protected by the freedom to provide services under European law.[20]

The CFR is also strongly influenced by the European Convention on Human Rights (ECHR), which applies equally to all EU Member States. Furthermore, when dealing with the legal framework applicable to medical AI, it is necessary to refer to the European Convention on Human Rights and Biomedicine (Oviedo Convention)[21] in the legal background consisting of fundamental rights treaties and conventions.[22] Even though the Oviedo Convention has found limited application in the pronouncements of the European Court of Human Rights[23] − which has also continued to refer to the ECHR for health issues − the Oviedo Convention remains the guiding star and minimum standard for interpreting fundamental rights in the medical field.[24] In 2019, the Council of Europe questioned the need to renew the reading of the Convention, interpreting it in the light of the challenges posed by new technologies, including the interference of AI in the doctor−patient relationship.[25] Most recently, the draft Council of Europe Convention on Artificial Intelligence (AI), Human Rights, Democracy and the Rule of Law was finalised at the last plenary of the Council of Europe's Committee on Artificial

[19] Brent Mittelstadt, 'The Impact of Artificial Intelligence on Doctor-Patient Relationship' (Council of Europe 2021); Kristina Astromskė, Eimantas Peičius and Paulius Astromskis, 'Ethical and Legal Challenges of Informed Consent Applying Artificial Intelligence in Medical Diagnostic Consultations' (2021) 36 *AI & Society* 509; Suzanne Kawamleh, 'Against Explainability Requirements for Ethical Artificial Intelligence in Health Care' (2023) 3 *AI and Ethics* 901; I Glenn Cohen, 'Informed Consent and Medical Artificial Intelligence: What to Tell the Patient?' [2020] *SSRN Electronic Journal* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3529576>, accessed 9 December 2024.

[20] Article 56 of the Treaty on the Functioning of the European Union (TFEU).

[21] Council of Europe, Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, Oviedo, 4 April 1997.

[22] Alessandro Mantelero, 'Regulating AI' in Alessandro Mantelero (ed), *Beyond Data* (Springer 2022).

[23] Francesco Seatzu and Fanni Simona, 'Corrigendum: The Experience of the European Court of Human Rights with the European Convention on Human Rights and Biomedicine' (2015) 31 *Utrecht Journal of International and European Law* 112.

[24] Laurence Lwoff, 'New Technologies, New Challenges for Human Rights? The Work of the Council of Europe' (2020) 27 *European Journal of Health Law* 335.

[25] Seppe Segers and Heidi Mertes, 'The Curious Case of "Trust" in the Light of Changing Doctor–Patient Relationships' (2022) 36 *Bioethics* 849; Mittelstadt (n 19).

Intelligence (CAI). The Convention is not dedicated to the healthcare field, but instead defines some rights and principles applicable to all AI systems. Nonetheless, the literature has already highlighted a possible health-oriented reading of the Convention, leading to very general conclusions.[26]

1.3 EU Secondary Law and GDPR

The academic literature has also dedicated considerable effort to analysing how EU secondary law applies to medical AI. Leading the academic literature are the topics of anti-discrimination law, and GDPR applied to the design and use of AI. While fundamental rights and antidiscrimination laws are not strictly intended as part of the product safety framework for medical AI, nonetheless, these sources guide the use of AI products and prescribe principles of conduct that are then translated into safety requirements. In this sense, antidiscrimination laws[27] and rights[28] entail that the development and operation of medical AI must be constantly and carefully checked to spot the presence or occurrence of bias.[29]

The GDPR has also been proven applicable to medical AI. More precisely, as a horizontal, risk-based, omnibus regulation that governs at the general level, the GDPR espouses broad principles that apply regardless of the particular context in which personal data is processed. Therefore, some specific articles of the GDPR apply to medical AI whenever these systems are engaged in the processing of personal data. Despite this, the GDPR is technology-neutral and, therefore, does not contain any reference to AI per se. Among these, the legal literature on GDPR has been focusing on the concept of transparency and accountability and how these principles coincide to shape the regulation of AI systems.

Referring to the existing literature[30] for a thorough analysis of the matter, it might be sufficient to highlight two main dispositions enshrined in Articles 22 and 13–15. Article 22 states that individuals ‘have the right not to be subject to a decision based solely

[26] Hannah van Kolfschooten and Carmel Shachar, ‘The Council of Europe’s AI Convention (2023–2024): Promises and Pitfalls for Health Protection’ (2023) 138 *Health Policy* 104935.

[27] Directive 2000/43/EC against discrimination on grounds of race and ethnic origin; Directive 2000/78/EC against discrimination at work on grounds of religion or belief, disability, age or sexual orientation; Directive 2006/54/EC equal treatment for men and women in matters of employment and occupation; Directive 2004/113/EC equal treatment for men and women in the access to and supply of goods and services; Directive Proposal (COM(2008) 462) against discrimination based on age, disability, sexual orientation and religion or belief beyond the workplace.

[28] CFR, Arts 20−26.

[29] Aiste Gerybaite, Sofia Palmieri and Francesco Vigna, ‘Equality in Healthcare AI: Did Anyone Mention Data Quality?’ (2022) 4 *Biolaw Journal - Rivista di BioDiritto* 385.

[30] ibid; Heike Felzmann and others, ‘Transparency You Can Trust: Transparency Requirements for Artificial Intelligence between Legal Norms and Contextual Concerns’ (2019) 6 *Big Data & Society* 205395171986054; Alexander J Wulf and Ognyan Seizov, ‘“Please Understand We Cannot Provide Further Information”: Evaluating Content and Transparency of GDPR-Mandated AI Disclosures’ [2022] *AI and Society*; Ronan Hamon and others, ‘Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making’ (2022) 17 *IEEE Computational Intelligence Magazine* 72.

on automated processing'.[31] Various authors have pointed out that this could be interpreted as either a right to object to such decisions or a general prohibition on significant algorithmic decision-making, therefore broadening or restricting the significance of the disposition according to the interpretation adopted. Either way, medical AI, such as AI-driven decision-support systems, would be affected by this provision unless the presence of a 'human in the loop' with substantial powers of assessment and intervention is ensured.[32] Further, in relation to automated decision-making, the GDPR gives a series of individual notifications and access rights specific to an automated decision, deriving from the principle of transparency and accountability.

Article 13 establishes a series of notification rights when information is collected directly from individuals.[33] A similar set of notification rights is established by Article 14 when information about individuals is collected from third parties.[34] Similarly, Article 15 establishes an individual right of access to information held by a company.[35] The three Articles share a common provision requiring disclosure of 'the existence of automated decision-making, including profiling'.[36] Additionally, this provision requires disclosure of 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject'.[37] Without diving into the very complex and partially unsolved debate of what constitutes an explanation,[38] it is sufficient to say that this provision would have a significant impact on medical AI regulation even without the implementation of the AI Act.[39] However, these dispositions applicable to data processing would not be fully implementable without the enforcement of design-related requirements. While providing an already interesting legal base for medical AI development and use, the full realisation of these principles is only possible when it is *technically* possible to realise them. In a sense, the AI Act operationalises these rights and principles, giving them a technical dimension through requirements applicable to AI's design.

[31] GDPR (n 6), Art. 22.

[32] In our case, the doctor would need to have substantial powers to understand and question the outcome. A mere observation of the AI decision process would not suffice.

[33] GDPR (n 6), Art. 13.

[34] GDPR (n 6), Art. 14.

[35] GDPR (n 6), Art. 15. See GDPR (n 6), Recital 63 (described as '[r]ight of access').

[36] GDPR (n 6), Arts. 13(2)(f), 14(2)(g) and 15(1)(h) (collectively, 'meaningful information' provisions).

[37] GDPR (n 6), Arts. 13(2)(f), 14(2)(g) and 15(1)(h).

[38] Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law*; Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law*; Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 *International Data Privacy Law*; Isak Mendoza and Lee A Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling' in Tatiana-Eleni Synodinou and others (eds), *EU Internet Law: Regulation and Enforcement* (Springer 2017).

[39] Nonetheless the added value of the AI Act over the GDPR is explained in the Guidance document 'AI and Personal Data A Guide for DPOs "Frequently Asked Questions"', Confederation of European Data Protection Organizations, June 2023.

The AI Act moves from this background, keeping fundamental rights (such as data privacy) as a legislative aim. More precisely, based on pre-evaluations of risks especially for health, safety and fundamental rights, the AI Act – unlike other product safety regulations – classifies the AI as a product in a different risk class.[40] The idea of the regulation of AI as a product is precisely to respond from design perspectives to the doubts concerning the development, operation and use of AI. Using safety requirements aimed at making the AI technically robust, the AI Act contributes to making AI systems trustworthy, i.e. safe, as it respects fundamental rights. In this sense, the AI Act offers better enforcement of fundamental rights since it relies on a solid horizontal market surveillance regulation. This system of market surveillance is flexible, and is linked with different types of Union harmonisation legislation structured along the NLF[41] approach, which contributes to regulating AI from the points of view of the different public interests protected by those Union legislations (e.g. health and safety, environment, protection of consumers, protection of fundamental rights, etc.).[42]

This paper focuses on the intertwining of these legislations, outlining the product safety framework applicable to AI systems in medicine. More specifically, since the major safety framework constituted by the AI Act and the MDR has already been analysed in the literature,[43] this paper aims to go a step further. While the literature to date has stopped at describing the regulatory interrelationship between the AI Act and the MDR, and emphasising the regulatory gaps, this paper aims to identify which regulations remain applicable to AI as a product when the AI Act is not applicable or − if applicable − does not provide for the application of safety requirements (the case of minimal risk AI). Hence, the following analysis is limited to analysing regulations that were created to regulate product safety − or that apply to AI as a product − in the *acquis* of the EU.

2. AI Act Classification System

The AI Act is intended to strike a proportionate balance between the need to protect persons from the potential harms of regulated products and the legislative aim of enhancing innovation and trade. Therefore, similar to other safety product regulations, the Act elaborates on a complex risk classification system based on the use of AI. According to foreseen risks that are connected to their intended use and context, AI systems have three risk classes. First, the AI Act presents a class of AI systems that are considered unacceptable because the amount or type of risks they

[40] Such as the MDR.

[41] The NLF is a common EU approach to the regulation of certain products such as lifts, medical devices, personal protective equipment and toys. See Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach' (2021) 22(4) *Computer Law Review International* 97.

[42] Gabriele Mazzini and Salvatore Scalzo, 'The Proposal for the Artificial Intelligence Act: Considerations around Some Key Concepts' [2022] *SSRN Electronic Journal* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4098809>, accessed 9 December 2024.

[43] Palmieri and Goffin (n 9).

present to safety, health and fundamental rights is unacceptable. The uses of AI systems that are considered unacceptable are carefully listed in Art 5 Title II.

Second, the high-risk AI class represents the heart of the regulation. As to the identification of the AI systems considered high risk, the AI Act uses a double ratio. On the one hand, the AI Act is based on and entwined with the NLF. The AI Act identifies high-risk AIs by referring to EU harmonisation legislation. According to Article 6 AI Act, to be considered high-risk AI, the AI systems have to be products or safety components covered by the harmonised legislation and simultaneously require a third-party assessment according to the same regulation. Following the mantra 'security by design',[44] the AI Act elaborates on some safety requirements that AI systems have to satisfy before, during and after being introduced in the EU market. The deal is that high-risk AI must comply with a set of safety requirements inherent, *inter alia*, to data governance and human oversight. Leaving aside a full description of the requirements and their analysis, it's sufficient to say that the final aim of these requirements is to ensure that the product placed on the market is safe and, following the EU's own logic, worthy of trust. On the other hand, identified high-risk systems used in certain contexts are considered to need particular precautions. These areas of use are listed in Article 6.2 and are further discussed in Section 2.2 below. Lastly, with the aim of always balancing safety and innovation, the AI Act identifies limited and minimal risk classes.

The limited risk class includes AI systems that, because of the context of use or the specific use made of the AI, pose specific risks already identified in the definition of this category. Included in this risk class are, for example, AI systems that generate or manipulate image, audio or video content to create deep fakes. Because of the specific risks they pose, the AI Act imposes on this class of AI transparency requirements aimed at making clear that the user is interacting with an AI system. The minimal risk class differs from the high risk class in being an open category. This means that all AI systems that − while respecting the definition of AI given by the AI Act − do not fall within the unacceptable, high or limited risk classifications fall in the minimal risk class. AI systems in this class are not subjected to any safety requirement since the risks they might present are minimal and, therefore, tolerable.

It is worth mentioning at this point the much-debated class of general-purpose AI or foundational models. The AI Act, as recently approved, contains a definition of general purpose AI (GPAI) models, identifying these as AI systems 'which ha[ve] the capability to serve a variety of purposes, both for direct use as well as for integration in other AI system'.[45] These models are trained with a large amount of data using self-supervision at scale and display significant generalisability. They are capable of competently performing a wide range of distinct tasks and can be integrated into a variety of downstream systems or applications. Additionally, the AI Act defines general-purpose AI systems as systems based on a GPAI model. These systems have the capability to

[44] Lee A Bygrave, 'Security by Design: Aspirations and Realities in a Regulatory Context' (2022) 3 *Oslo Law Review* 126.

[45] AI Act, Art. 3(66).

serve a variety of purposes, both for direct use and for integration into other AI systems.

Chapter V, which is entirely devoted to general-purpose AI, and Article 51 in particular provides classification criteria. In this respect, the classification to which general purpose AIs are subjected is not in terms of risk classes, but rather concerns the possibility that general purpose AI presents 'systemic risks'.

For general purposes, AI that does not present systemic risks has to satisfy some transparency requirements. All providers of AI models under the Global Partnership on Artificial Intelligence are required to create and maintain updated technical documentation. This documentation must be made available to downstream AI system providers. Additionally, all providers of GPAI models must implement a policy to abide by Union copyright law. This includes using state-of-the-art technologies like watermarking to ensure lawful text- and data-mining exceptions are carried out as envisioned under the Copyright Directive.[46] Furthermore, GPAI models must create and publish a detailed summary of the content used during the training process. The AI Office provides a template for this summary to ensure it contains sufficient information. It should be noted that if a company is located outside of the EU, it is required to appoint a representative within the EU. However, AI models made available through a free and open source will be exempt from certain obligations, such as the requirement to disclose technical documentation, provided they are likely to impact research, innovation and competition positively.

Models created by general purpose AI (GPAI) with 'high-impact capabilities' could be a potential threat to the internal market. This is due to their extensive reach and their adverse effects on public health, safety, security, fundamental rights and society. Therefore, GPAI providers must notify the European Commission if their model is trained using a total computing power exceeding 10^25 FLOPs (i.e. floating-point operations per second). When they exceed this threshold, it will be presumed that the model is a GPAI model posing systemic risks.[47] Whenever a GPAI is identified as presenting systemic risks, the manufacturer must comply with a different set of requirements in addition to the provisions on transparency and copyright protection. Systemic-risk GPAI models providers must continuously assess and reduce the risks they pose and ensure cybersecurity protection. This entails various actions, such as

[46] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance).

[47] According to the brief on the AI Act elaborated by Tambiama Madiega, (<https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf>), FLOPs measure a computer's processing speed. The threshold should be adjusted over time to reflect technological and industrial changes. Moreover, the Commission is entitled to take individual decisions designating a GPAI model as posing systemic risk if it is found that it has capabilities or impact equivalent to those captured by the FLOP threshold on the basis of an overall assessment of criteria (e.g. quality or size of the training data set, number of business and end users, degree of autonomy and scalability). In the USA, President Biden's AI executive order set 10^26 FLOPs as the threshold for AI models that need to be reported to the government along with details of their training, capabilities and security.

monitoring, documenting and reporting severe incidents such as violations of fundamental rights. Additionally, corrective measures must be implemented to address any issues that may arise.

2.1 What We Already Know: the Tortuous Relationship between the MDR and the AI Act

The legal literature makes it clear that the AI Act does apply to medical AI. More precisely, the AI Act applies to medical AI systems mainly through the reference made to the MDR and the In Vitro Device Regulation (IVDR),[48] which is mentioned among the harmonised rules in Annex I of the AI Act.

Reference should be made to the existing literature for a more in-depth analysis of the intertwining between the classification systems of the AI Act and the MDR/IVDR, but here it is sufficient to recall that the AI Act classification, when applied to medical AI, relies heavily on the classification presented in the MDR and IVDR. The MDR and IVDR first identify the definition of medical devices and in vitro devices, distinguishing these from other devices on the basis of the function these medical devices are supposed to perform. Once identified as a medical device, the two Regulations present risk classifications based on the intended uses of the device. More precisely, the Regulations identify specific characteristics of the device combined with its intended use. For example, one relevant factor is the length of contact between the body and the device, with this consideration being one, amongst many, that is ultimately used in determining the risks associated with the device. Based on these features, the Regulations identify the class of reference for the device under scrutiny.

According to the class in which the medical devices (MD) or in vitro medical devices (IVD) fall, the dispositions of the two Regulations apply in different ways. For this analysis, two aspects are of special note. Regardless of the class in which the MD/IVD falls, the requirements set out by the MDR and IVDR remain applicable. What changes is the permeance of the scrutiny to which the devices are subjected. In the case of class I devices,[49] the manufacturer is solely responsible for compliance with the requirements of the Regulations; in the case of class IIa, IIb and III devices,[50] the scrutiny is conducted by a third-party authority.[51]

The AI Act approach is similar yet different. Still starting with the definition of AI systems, the AI Act, similarly to the MDR and IVDR, discerns an AI product from other

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

[49] Or class A under the IVDR.

[50] To keep this discussion concise, it is sufficient to note that the classification of medical devices is determined by the manufacturer based on their intended use and risk level, while Notified Bodies and regulatory authorities are responsible for verifying the classification through conformity assessments and inspections. For a more detailed exploration of this topic, the reader is referred to the literature from Palmieri and Goffin (n 9).

[51] In case of the IVDR, Classes A, B, C and D.

products present in the market thanks to a much-debated definition of 'AI systems'.[52] The AI Act identifies risk classes following the methods mentioned above (mainly referring to harmonised rules in annex I). In relation to medical AI, the classification of the AI Act is implemented thanks to the prior classification made through the medical device and in vitro device classifications. Medical devices that, because of their features, end up in a higher class of risk under MDR and IVDR – and therefore are subjected to third-party authority— will be classified as high-risk AI systems. Conversely, those devices presenting lower risks under the MDR and IVDR will most likely fall into the minimal or limited risk class following the AI Act classification.

2.2 The Often-Overseen Annex III

Article 6(2) AI Act opens another door for the regulation of medical AI. Through reference to the context of use listed in Annex III therein, the AI Act adds another criterion to identify medical AI as high risk. More precisely, Annex III point 5 identifies three areas that might be relevant for our analysis:

> (a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for essential public assistance benefits and services, including healthcare services, as well as to grant, reduce, revoke, or reclaim such benefits and services;
>
> […]
>
> (c) AI systems intended to evaluate and classify emergency calls by natural persons or to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by police, firefighters and medical aid, as well as of emergency healthcare patient triage systems;
>
> (d) AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance.

While health and healthcare are not among the contexts of use and use cases listed in Annex III, these provisions might still be relevant for medical AI, for example in a field that might not fit into the definition of a medical device or a low-risk medical device, and therefore fall into the AI Act's minimal risk class.

However, while evaluating the relevance of these sections for the elaboration of a safety framework for medical AI, there are two important considerations. First, these paragraphs apply to medical AI depending on the definition we adopt of 'medical AI'. As discussed in Section 1.2 above, we might decide to include in this category only AI-powered medical devices or, rather, as in this paper, adopt a more extensive interpretation. Adopting this second approach, we might include in the definition of medical AI systems that are not medical devices but that contribute to the healthcare ecosystems through essential or ancillary tasks. Annex III point 5(a), for example, might

[52] Luca Bertuzzi, 'EU lawmakers set to settle on OECD definition for A' (Euractiv, 7 May 2023) <https://www.euractiv.com/section/artificial-intelligence/news/eu-lawmakers-set-to-settle-on-oecd-definition-for-artificial-intelligence/>, accessed 19 July 2024.

contribute to regulating AI systems used to evaluate the right to access healthcare services. This is the case, for example, of healthcare systems employed in immigration policies used to assess whether an immigrant, due to his or her status, has access to certain treatments under the healthcare systems of a certain Member State. While not a medical device, this kind of system has a strong impact on healthcare organisations and the patient's fundamental rights, potentially leading to discrimination in access to healthcare due to bias inherent to the functioning of AI systems.[53] The same goes for the systems identifiable thanks to Annex III point 5(d) evaluating the eligibility of a person's health and life insurance. Although not classified as medical devices, these systems might seriously impact an individual's healthcare experience to the point of excluding them from accessing healthcare. Lastly, point (c) allows for the regulation of many AI systems already used in the healthcare ecosystem to more efficiently perform patient triage[54] or to handle incoming emergency calls.[55]

Secondly, the AI falling into these contexts of use should not be considered high risk *tout court*. According to Article 6(2), they shall be considered high risk if they pose a significant risk to health, safety and fundamental rights (or, in specific cases, to the environment). The AI Act puts on the Commission the onus of providing guidelines to specify when an output of those AI systems listed in Annex III would pose a significant risk to health, safety and fundamental rights. According to the Act, this task must be fulfilled six months before the Act enters into force. Despite the appreciable effort of the EU Commission in clarifying the matter, this timeline allows manufacturers little time to adapt their systems to the eventual requirements applicable. Furthermore, until then, we are left to wonder if these provisions will concur with the safety framework for medical AI.

3. Shortcomings of the AI ACT and MDR's Interweaving

Despite the AI Act providing for a regulation − a safety framework also applicable to medical AI − this framework might be of limited *significance*.[56] As already shown in the literature, the influences and interconnections between the AI Act and the MDR/IVDR leave open the possibility for undesirable loopholes. In other words, despite the AI Act

[53] Mittelstadt (n 19).

[54] Chris Kim and others, 'An Automated COVID-19 Triage Pipeline Using Artificial Intelligence Based on Chest Radiographs and Clinical Data' (2022) 5 *npj Digital Medicine*; Sean Delshad, Venkata S Dontaraju and Vipindas Chengat, 'Artificial Intelligence-Based Application Provides Accurate Medical Triage Advice When Compared to Consensus Decisions of Healthcare Providers' [2021] *Cureus*; Maree Hitchcock and others, 'Triage: An Investigation of the Process and Potential Vulnerabilities' (2014) 70 *Journal of Advanced Nursing* 1532.

[55] European Stroke Organization, 'AI tool outperforms human emergency call handlers' (Healthcare in Europe.com, 24 May 2023), <https://healthcare-in-europe.com/en/news/ai-tool-emergency-call-handlers-stroke.html>, accessed 19 July 2024; S. Hughes, 'AI Improves Stroke Recognition in Emergency Calls' (Medscape, 24 August 2023), <https://www.medscape.com/viewarticle/992515#:~:text=The%20AI%20model%20was%20trained,to%20be%20actual%20stroke%20cases>, accessed 19 July 2024; see also the results of the Horizon 2020 funded project 'AI4EMS' <https://cordis.europa.eu/article/id/421437-artificial-intelligence-detects-cardiac-arrest-in-emergency-calls>.

[56] Palmieri and Goffin (n 9).

largely applying to medical AI for the mere fact that these systems reflect the definition of AI given by the AI Act and of medical devices by the MDR, they might not be subjected to the AI Act requirements since they end up in the minimal risk class. Therefore, despite the fact that the AI Act is applicable *en tant que tel*, it fails to provide these systems with the regulatory backing to accomplish its *raison d'être*, protecting fundamental rights, health and safety through safety requirements from the potential hazards of AI uses. The reason is clear: through the complex risk evaluation carried out on the back stage of the AI Act, these AI systems seem to be harm-free or to minimise the potential for possible harm. Still, as Hauglid and Mahler explain,[57] minimal-risk (medical) AI might pose risks to health, safety and fundamental rights. Thus, AI systems that, according to the AI Act's inner evaluation, are of very limited relevance might turn out to be rather risky in daily use.

However, the AI Act arises within a complex and dynamic legal background. The AI Act is not detached from this background. On the contrary, the Act is strongly interwoven with other legal documents, as already shown through the analysis of the influences between the MDR and the AI Act. The MDR is certainly not the only legal text that completes the puzzle of the safety framework for medical AI. As already highlighted in the some previous work of these authors, other regulations might concur, from different angles, to create the safety framework for medical AI, imposing 'external' requirements even when the AI Act classification system would exclude the applicability of the AI Act's requirements. From here originates the challenge of mapping which regulations, if any, apply to systems that are minimal-risk medical AI or that, for other reasons, do not have to comply with the AI Act requirements.

The following sections highlight the cases in which medical AI, following our understanding of the term, might, for different reasons, escape the AI Act safety requirements. I will then summarise the applicable legal framework concurring to ensure the safety of the medical AI systems.

3.1 AI Systems Exempted from the AI Act Requirements

As previously mentioned, the AI Act provides a framework consisting of safety requirements, the application of which is limited to high-risk AI. In the cases so far discussed, medical AI, which also consists of medical devices of high-risk classes, needs to satisfy the safety requirements both before entering the market and while being actively distributed in the marketplace. In these cases, the AI Act makes a significant contribution to the safety framework of medical AI. However, in other cases, the AI Act does not contribute to the safety of medical AI. This might happen for different reasons. Firstly, and most notoriously, when an AI system, while being a medical device, does not enter into one of the higher-risk classes under the MDR. According to the intertwining between the AI Act and MDR,[58] some medical AI falling into class I of the MDR will be classified in the AI Act as minimal risk. The AI Act requirements will not apply to these systems. This also goes for other AI systems used in healthcare or with functions ancillary to health and well-being that do not meet the definition of the

[57] (n 9).

[58] Although the argument also applies to the IVDR, this article will refer only to the MDR.

medical device. This is the case of the devices excluded from the definition of medical device according to paragraph 19 MDR, or devices that do not meet the intended uses of Article 2 MDR.

These systems are still subjected to the AI Act for the mere fact of mirroring the definition of 'AI system' outlined by the AI Act. Nonetheless, they will not be subjected to the safety requirements, leaving the AI Act applicability of very little significance.

3.2 Sideways to the AI Act High-risk Class?

While exploring the possible applicable safety framework for medical AI, an examination of Article 6 of the AI Act is also useful. As explained above, Article 6 refers to EU harmonised rules stating that when a device is categorised as a product or as a safety component in one of these rules – and as such needs to comply with a third-party assessment – the system is to be considered high-risk.

We have seen how this works for medical AI, fulfilling one of the intended uses presented in the MDR. In this sense, the MDR is the main 'co-regulator' of medical AI, meaning that thanks to the interplay between MDR and the AI Act, medical AI finds a rather tailored safety framework. Nonetheless, one might wonder if medical AI might be a product or a safety component under other harmonised rules listed in Annex I. In particular, it is of interest to understand whether, when a medical AI is not a medical device and therefore not getting into the high-risk class following this 'classification path', the device might still be classified as high risk through the reference to another harmonised rule.

Among the regulations listed therein, the Machinery Regulation[59] warrants particular attention thanks to the references made to this Regulation concerning smart medical robots (SMR).[60] SMRs are not a simple entity to define, as pointed out by the European Parliament in 2017.[61] On the contrary, they are described by the features and tasks they perform.[62] SMRs bring together the physical and digital worlds, raising questions about how this works from a regulatory point of view. These devices are subjected to the MDR when performing one of the functions fitting the definition of 'medical

[59] Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC.

[60] Eduard Fosch-Villaronga and Tobias Mahler, 'Cybersecurity, Safety and Robots: Strengthening the Link between Cybersecurity and Safety in the Context of Care Robots' (2021) 41 *Computer Law & Security Review* 105528; Tom Goffin and Sofia Palmieri, 'Regulating Smart Healthcare Robots: The European Approach' in *Research Handbook on Health, AI and the Law* (Edward Elgar Publisher 2024).

[61] Civil Law Rules on Robotics European Parliament resolution of 16 February 2017 with recommendation ons to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0051&rid=9>.

[62] Erica Palmerini and others, 'RoboLaw: Towards a European Framework for Robotics Regulation' (2016) 86 *Robotics and Autonomous Systems* 78.

device'.[63] In most cases, SMRs fit the definition of a medical device while performing a function related to therapy. In this case, the (robot) medical AI might be called to comply with the MDR, the Machinery Regulation – in relation to its physical components – and eventually the AI Act.[64] In this case, they would fall in one of the AI Act's risk classes according to the interplay between the AI Act and MDR.

Some robots act as social companions or perform care functions, not fitting the medical device criteria, but still very much linked to a broader understanding of healthcare. It is possible to wonder whether, in these cases – when the MDR does not apply – the reference to the Machinery Regulation in Annex I might still allow the classification of SMRs as high risk in the AI Act and, therefore, comply with the safety requirements.

For this to be true, the AI system should, as already mentioned, be a product or a safety component regulated under the Machinery Regulation. The Machinery Regulation applies to machinery intended as 'an assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application'.[65] According to this definition, AI systems could play two different roles while embedded in a machinery product: an integrated component of the machinery; or a safety component.

In these cases, the same reasoning applies to the AI product covered by the Machinery Regulation as for the AI systems covered by the MDR. In other words, the AI system included in the Machinery Regulation may certainly fall under the AI Act, but it will have to be a high-risk AI system to be covered by the safety requirements therein. For this to happen, not only must the device be part of the Machinery Regulation, but it must also undergo third-party assessment.

This brings us to the question of which machinery (i.e. whether it contains an AI system) must satisfy a third-party assessment. The various conformity assessment procedures are found in Annexes VIII, IX and X of the Machinery Regulation. The rules for their selection are found in Article 12. Generally, if the machinery is not covered by Annex IV (i.e. does not present higher risks), the manufacturer must apply the conformity assessment procedure with internal checks on the manufacture of machinery (Annex VIII). This procedure does not require the intervention of a third party. For the categories of machines listed in Annex IV (i.e. machines with higher risks), the conformity assessment procedure for Annex IV machines must involve a third party (i.e. a 'notified body'). We can therefore conclude that the requirements of the AI Act apply to those AI systems that are not medical devices but are integrated into a machinery product among those subject to third-party assessment according to Annex IV. Whether this complex regulatory 'ping-pong' means that many AI systems that are components of machinery products are subject to the requirements of the AI

[63] Eduard Fosch-Villaronga and Hadassah Drukarch, *AI for Healthcare Robotics* (Taylor & Francis Ltd 2022).

[64] Goffin and Palmieri (n 60).

[65] Machinery Regulation, Art. 3(1).

Act is difficult to say without analysing a concrete case. Nonetheless, this relationship between the AI Act and machinery regulation opens up possible horizons for the safety regulation of AI as a product.

Another scenario is when the AI system might be classified as a safety component under the Machinery Regulation and, as such, be considered high risk under the AI Act. ‘Safety component’ is defined in the Machinery Regulation as follows:

[A] physical or digital component, including software, of machinery which serves to fulfil a safety function and which is independently placed on the market, the failure or malfunction of which endangers the safety of persons but which is not necessary in order for the machinery to function or may be substituted by normal components in order for the machinery to function[.]

The Machinery Regulation gives a clear and concise description of the legal profile applicable to AI systems used as safety components. According to Recital 45, ‘software ensuring safety functions of machinery based on artificial intelligence, embedded or not in the machinery product, should be classified as a high-risk machinery product […]’.[66] Therefore, the conformity assessment of software, which ensures safety functions based on AI, should be carried out by a third party. As a consequence, AI systems that perform a safety function in a machinery product – being a product covered by the Machinery Regulation and being always subject to a third-party assessment – will have to satisfy the requirements prescribed in the AI Act for high-risk systems.

4. Other Applicable Regulations

The cases discussed above raise the question whether these systems are free of safety requirements because of the failure of the AI Act safety architecture, or if, despite not being covered by the AI Act, a safety framework may be grounded in other European regulations.

This section maps other legislation that potentially contributes to the safety of medical AI.

4.1 Medical Device Regulation

In cases where the AI Act is not applicable even through reference to the Machinery Regulation, medical AI can still find a safety framework through other legislation. First is the aforementioned MDR, which offers a safety framework for medical AI in its own right, and not only in relation to the AI Act. As already explored in a previous work of these same authors, the MDR applies to AI following the specific provision dedicated to software.[67]

[66] In a more nuanced way, Recital 20 of the Machinery Regulation states that ‘in view of the essential protective function they perform, certain components included in the indicative list of safety components in Annex II should also be subject to conformity assessment procedures and listed in Annex I’.

[67] Namely, MDR, Rule 11.

According to the MDR, Rule 11, software is regulated and classified in its own right. Because the MDR has a considerable focus on software, some stakeholders have considered it to provide a sufficient safety framework for medical devices, even without burdening the manufacturers with additional requirements.[68] Although the purpose of the AI Act is to give broader protection in both the scope of application and intensity of requirements, and to tackle uncovered issues − such as continuous learning of the AI models or the identification of algorithmic biases[69] − the MDR relevance for medical AI certainly remains a pivotal evaluative framework for minimal-risk AI, on which the AI Act does not place requirements. Of particular note is that, despite sharing the risk-based approach with the AI Act, the MDR applies its general safety and performance requirements to all the classes identified in the Regulation. The appearance of a lower- or higher-risk class mainly entails the degree of scrutiny over the safety requirements' compliance, i.e., the compliance of low-risk (class I) medical devices is assessed only by the manufacturer, while for higher-risk classes, a third-party authority is involved in the evaluation.

Nonetheless, without focusing on the appropriateness of this 'softer' conformity assessment, it is sufficient here to recall that for AI systems of limited and low risk, the safety requirements of MDR Annex I remain applicable as a sector-specific safety framework.

4.2 The General Safety Product Regulation

While discussing the complex intertwining of regulations that participate in the safety framework for medical AI, it is essential to mention the GPSR. In May 2023, the GPSR was published in the *Official Journal* of the EU, replacing the General Product Safety Directive.[70] The GPSR seeks to address the product safety challenges of emerging technologies, including the use of AI. Allegedly, the proposed text would simplify the EU's legal framework for product safety, in particular, by including references to pivotal EU regulations, such as the Regulation on Market Surveillance[71] and the AI Act.

The GPSR aims to create a single set of market surveillance rules for both harmonised and non-harmonised products by aligning the provisions with the Market Surveillance Regulation. The GPSD requires that all non-food consumer products placed on the

[68] Alexander Olbrechts, 'How the AI Act Could Unintentionally Impact Access to Healthcare' (*Euractiv*, 1 March 2023), <https://www.euractiv.com/section/digital/opinion/how-the-ai-act-could-unintentionally-impact-access-to-healthcare/>, accessed 19 July 2024.

[69] Hannah van Kolfschooten, Janneke van Oirschot and Nicastro Claudia, 'Five Big Medtec Myths about Medical AI Debunked' (*HAI, 2022*), <https://haiweb.org/five-big-medtech-myths-about-medical-ai-debunked/>, accessed 19 July 2024.

[70] Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (Text with EEA relevance).

[71] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA relevance).

internal market are safe and function as a 'safety net'. It applies fully to non-harmonised products, as well as to those aspects of product safety of harmonised products that are not covered by the Market Surveillance Regulation or by harmonising legislation.

In a 2021 briefing, the European Parliament[72] stated that it was still not clear to what extent the GPSD applies to new technologies, such as AI.[73] In response, Digital Europe[74] argued that any safety issue caused by the use of AI should be addressed within the existing sector-specific regulations – such as the AI Act – leaving the GSPR an ancillary role.[75]

In addition, the relationship between the two Regulations is better explained in the Preambles of both the GSPR and AI Act. Recital 1(3) of the AI Act recalls the White Paper on AI stating that the Act is part of 'a comprehensive package of measures that address problems posed by the development and use of AI' and therefore 'consistency and complementarity is [...] ensured with other ongoing or planned initiatives of the Commission that also aim to address those problems, including the revision of sectoral product legislation (e.g. the Machinery Directive, the General Product Safety Directive)[…]'. Furthermore, Recital 8(2) of the AI Act states that '[...] AI systems related to products that are not high-risk by this Regulation and thus are not required to comply with the requirements set out herein are nevertheless safe when placed on the market or put into service. To contribute to this objective, the Directive 2001/95/EC[76] of the European Parliament and the Council would apply as a safety net'.[77]

The GPSR proposal[78] as drafted by the EU Commission mentioned its consistency with other legislative acts, such as the AI Act. The Preamble of the proposed GPSR disposed the consistency of the Regulation with other EU policies and clarified its relationship with the AI Act, specifying that the GPSR '[...] takes into consideration these provisions and provides a safety net for products and risks to health and safety of consumers that do not enter into the scope of application of the AI proposal'; and, more specifically, that the AI Act acts as a horizonal framework aimed to focus on high-risk applications.[79] Consequently, concerning product safety, the AI Act will function as sectorial legislation, establishing specific requirements for AI − more specifically for high-risk

[72] Clément Evroux, 'General product safety regulation' (EPRS, 2023).
[73] The Briefing mentions that the GPSD study also identified an issue with products involving machine learning and AI, as these can evolve over time.
[74] Evroux (n 72), p 8.
[75] Evroux (n 72).
[76] The Directive 2001/95/EC is the previous version of the GPSR, now replaced by Regulation (EU) 2023/988.
[77] Marco Almada and Nicolas Petit, 'The EU AI Act: Between Product Safety and Fundamental Rights' [2022] SSRN: <https://ssrn.com/abstract=4308072>.
[78] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council.
[79] Ibid, para 1.5.4.

systems − and 'this proposal will apply as a safety net for products and aspects not covered by other sectorial legislation to provide a legal basis for withdrawing such products to ensure an effective protection of consumers'.[80]

However, considering the adopted text of the GPSR, we are left with two significant questions. In the final version of the GPSR, the text is less clear on the role played by this Regulation. In particular, it is unclear whether low-risk AIs, to which the Act per se applies, but to which no security requirements apply, should be considered subject to the GPSR. In a favourable direction would seem to be Recital 6, which states that the GPSR would respond to the need for a broad legislative framework of a horizontal nature to fill gaps and complement provisions in existing or future sectoral Union harmonisation legislation, and to ensure consumer protection not otherwise covered by such legislation, in particular, to achieve a high level of consumer health and safety protection. However, where such products are subject to 'specific safety requirements imposed by Union law, this Regulation applies only to those aspects and risks or categories of risks not covered by those requirements'.[81]

This provision can be interpreted in two ways. On the one hand, it could open up the applicability of the GSPR to minimal-risk AI, given that the risks assumed are not covered by any safety requirements under the AI Act. However, on the other hand, the question must be asked whether the risks potentially presented by minimal-risk AI are not the same risks that the safety requirements of the AI Act seek to mitigate but that escape the applicability of those requirements due to an erroneous initial assessment of the dangerousness of the AI device. Adopting this second interpretation, the risks presented by the AI minimal risk system would be of the same 'category' as those that the AI Act seeks to contain, excluding the residual applicability of the GSPR.

Moreover, underneath these considerations of an interpretative nature there remains a margin of doubt as to the overall applicability of the GPSR to the health sector in which the AI is used. In other words, it must be remembered that the GPSR applies to products 'intended for consumers or [...] likely, under reasonably foreseeable conditions, to be used by consumers even if not intended for them'.[82] The question arises as to whether, in cases of AI use in the medical field, the patient can be perceived as a 'consumer'. In the GPSR, the consumer is defined as 'any natural person who acts for purposes which are outside that person's trade, business, craft or profession', placing no *ex litteris* obstacles in the way of bringing the role of patient closer to that of the consumer. Moreover, due to the evolving marketisation of healthcare,[83] the

[80] Ibid para 1.5.4.

[81] GSPR, Art. 2(2).

[82] GSPR, Art. 3.

[83] Nick Krachler, Ian Greer and Charles Umney, 'Can Public Healthcare Afford Marketization? Market Principles, Mechanisms, and Effects in Five Health Systems' (2022) 82 *Public Administration Review*; Katy Mason and Luis Araujo, 'Implementing Marketization in Public Healthcare Systems: Performing Reform in the English National Health Service' (2021) 32 *British Journal of Management*; Therese Feiler, Joshua Hordern and Andrew Papanikitas, *Marketisation, Ethics and Healthcare: Policy, Practice and Moral Formation* (Routledge, 2018).

patient increasingly plays a role comparable to that of a consumer.[84] Identifying the patient as a consumer of healthcare services would allow the GPSR to apply, at least in theory, to medical AIs when they are offered in the healthcare service of which the patient is a consumer, ultimately allowing the safety requirements of the GSPR to apply to medical AIs.

4.3 Cybersecurity Regulations

Some requirements of the AI Act are dedicated to the strengthening of the cybersecurity of AI systems. Whenever the AI Act requirements are not applicable, we must look instead for cybersecurity requirements applicable to medical AI. Highly relevant for our analysis are the Cybersecurity Act (CSA),[85] the Network and Information Security Directive (NIS 2) and the Cybersecurity Resilience Act.

Together with strengthening the role of the EU Agency for Cybersecurity (ENISA), the CSA created a cybersecurity certification framework for some products and services. This framework provides a comprehensive set of rules, technical requirements, standards and procedures based on the evaluation of the security properties of a specific ICT-based product or service. It will attest that ICT products and services that have been certified by such a scheme comply with specified requirements.

The CSA clarifies that the healthcare sector should be one of its priorities[86] and applies to medical AI as long as it conforms to the definition of 'ICT product' presented in its Article 2(12). When the medical AI is a medical device, some stakeholders have questioned the applicability of the CSA rules and the operability of the therein-enforced European cybersecurity certification schemes (ECCS) for healthcare.[87]

As discussed by Biasin and Kamenjasevic,[88] these concerns were mainly focused on the imperfect overlap between MDR and cybersecurity certification schemes and requirements.[89] In the case of medical devices, the two certifications might have introduced some duplications in the requirements the manufacturers have to comply with.[90]

[84] Paul Vigario, 'Patients as Consumers Are Changing the Health Care Industry' (*Medical Economist*, 28 February 2023).

[85] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance).

[86] CSA, Recitals 1 and 15.

[87] See, e.g., COCIR, 'Advancing Cybersecurity of Health and Digital Technologies' (2019), <https://www.cocir.org/uploads/media/19036_COC_Cybersecurity_web.pdf>, accessed 19 July 2024.

[88] Elisabetta Biasin and Erik Kamenjasevic, 'Cybersecurity of Medical Devices: Regulatory Challenges in the EU' *SSRN Electronic Journal* (2021), <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3855491>, accessed 9 December 2024.

[89] ibid.

[90] See Biasin and Kamenjasevic (n 88) for further insight on this matter.

In contrast, for medical AI that does not meet the definition of a medical device, the CSA might apply as a safety net when no other regulations are applicable.[91] However, the CSA certification is voluntary unless otherwise specified in other EU law or national law, and therefore does not represent a strong regulatory contribution to the safety framework for medical AI. On the contrary, several EU regulation proposals, such as the NIS 2 and Cyber Resilience Act, might present mandatory cybersecurity requirements for medical AI.

The NIS 2 is the main piece of the EU-wide legislation on cybersecurity, established to achieve a high common level of cybersecurity across the Member States. Formally adopted by the Parliament and the Council in November 2022 and entered into force on 16 January 2023, the NIS 2 strengthens security requirements, addresses the security of supply chains, streamlines reporting obligations, and introduces stricter supervisory measures and enforcement requirements. According to Article 1(2)(b) NIS 2, the Directive lays down 'cybersecurity risk-management measures and reporting obligations for […]' identified entities. Compared to its predecessor, the NIS Directive, the NIS 2 has a broader scope of application, including new entities called to comply with it**,** with a significant impact on the healthcare sector.[92] Within the scope of the regulation as 'essential entities', we find healthcare providers, together with other new-entry entities, relevant to the healthcare sector. Among these essential entities, the NIS 2 includes EU reference laboratories, entities carrying out research and development activities for medicinal products, entities manufacturing basic pharmaceutical products and preparations, and manufacturers of medical devices considered critical during a public health emergency.[93] Furthermore, among the 'important entities' to which the Directive continues to apply, the proposal includes the 'entities manufacturing medical devices and in vitro diagnostic medical devices'.[94]

Thanks to these changes, the NIS 2 is now applicable to AI systems even where the AI Act requirements are not applicable, such as in the case of class I medical devices. Similarly, the NIS 2 might be applicable for those devices that might be linked to one of the essential or important entities identified in the Directive in Annexes I and II. This might be the case of medical AI used within laboratory research or research on pharmaceutical products, but not fitting the definition of a medical device.

To complement this already rich regulatory framework, it is essential to mention the Cyber Resilience Act. According to Article 1, the Cyber Resilience Act lays down rules to ensure the cybersecurity of products released on the internal market that are not covered by sectoral regulations. The products to which the Act is applicable are those 'with digital elements whose intended or reasonably foreseeable use includes a direct

[91] Elisabetta Biasin and Erik Kamenjašević, 'Cybersecurity of Medical Devices: New Challenges Arising from the AI Act and NIS 2 Directive Proposals' (2022) 3 *International Cybersecurity Law Review* 163.

[92] Biasin and Kamenjašević (n 86).

[93] European Commission 'Combined evaluation roadmap/inception impact assessment revision of the NIS directive' (2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:Ares(2020)3320999&from=EN>, accessed 8 February 2022.

[94] NIS 2, Annex II (5)(a).

or indirect logical or physical data connection to a device or network' excluding, among others, systems such as (in vitro) medical devices. This system shall be placed on the market only when meeting the cybersecurity requirements set out in Annex I.[95] In particular, Annex III of the Cyber Resilience Act identifies some products to be considered 'critical products' because of the impact of their cybersecurity vulnerabilities or because of the sensitivity of the environment in which they are intended to be used. Annex III mentions at least one 'critical product' relevant to our analysis. 'Robot sensing and actuator components and robot controllers'[96] lead us back to the already mentioned SMRs. We might presume that some AI systems involved in the SMR functioning – which do not fall into the high-risk class of the AI Act, because they are not medical devices of the high-risk class or because it is not a safety component of a robot –might still see some applicable cybersecurity requirements when used to give the robot AI-powered sensing capabilities and skills to interact with the environment.

5. Conclusions

In 2020, Schneeberger et al. concluded their paper by arguing that the then-legal framework for medical AI was a technologically neutral regulation; that is, it applies to AI despite AI not being the main object of the regulation. In only a few years, the regulatory landscape has changed considerably. We now see many legislative initiatives to regulate issues previously unaddressed relating to the development and use of AI, or to renew and amend existing regulations with AI as the ultimate legal challenge in mind.

While it is true that, as stakeholders often complain, medical AI is not at the centre of regulatory production and does not benefit from *ad hoc* measures, there is nevertheless a broad spectrum of regulations applicable to medical AI that go far beyond the AI Act and the MDR. We have seen that when the AI Act fails to give a solid safety framework, other regulations addressing the safety of products find application. Therefore, even where the AI Act requirements do not have to be satisfied, other safety requirements might need to be applied according to the type and use of the AI system under scrutiny.

Moreover, the AI used in medicine certainly benefits from the overall vision adopted by the EU. This approach, based on human-centeredness, aims to frame the use and development of AI systems in an ecosystem of trustworthiness. This approach fits well with the underlying principles of medical practice and thus facilitates the blending of technology, regulation and medicine.

[95] Cyber Resilience Act, Art. 5.

[96] Annex III, Class II, point 14.