

ARTICLE

Regulatory Approaches Towards AI-Based Medical Device Cybersecurity: A Transatlantic Perspective

Elisabetta Biasin  and Erik Kamenjašević 

Centre for IT & IP Law, KU Leuven Faculty of Law and Criminology, Leuven, Belgium

Corresponding author: Elisabetta Biasin; Email: elisabetta.biasin@kuleuven.be

Abstract

Cybersecurity of medical devices has become a concrete concern for regulators and policymakers in the European Union and United States. Following the COVID-19 pandemic, there has been an increase in cyber-attacks on critical healthcare infrastructures and their IT systems, which have suffered service disruptions and put patients' health and safety at risk. The increase in cyberattacks on healthcare infrastructure, including medical devices, exacerbated by the growing digitalisation of healthcare services in the EU and the US, has led legislators and regulatory bodies to pay more attention to cybersecurity. Cybersecurity of AI-based medical devices requires the assessment of three areas subject to evolving regulatory approaches: medical devices, Artificial Intelligence (AI), and cybersecurity. Although they may appear distinguished in regulatory matters, the existence of AI-based medical devices and their possible cyber vulnerabilities makes clear that the three are intertwined and deserve closer attention from a regulatory point of view. Few scholars have devoted attention to AI and cybersecurity together. Even less, in our understanding, few comprehensive and EU/US comparative pieces of literature reflect on this specific issue. This paper aims to fill this gap and address the main implications of different regulatory approaches toward AI medical device cybersecurity in the EU and the US. The research stems from the assumption that regulation of medical devices in the EU has been historically inspired by regulatory trends in the US, although with the different cultural, societal, and legal traditions that made them adapt to the specificities of the territory. The paper observes that the US is a rule-based system reflecting a "command-and-control" approach, while the EU system is a principle-based one. While they share the main characteristic of being risk-regulation-based systems, their differences impact how AI-enhanced cybersecurity is regulated.

Keywords: artificial intelligence; cybersecurity; EU/US; medical device; regulation

I. Introduction

I. AI-based medical devices cybersecurity

Cyberattacks on healthcare infrastructures may concern AI-based medical devices as part of their IT systems (for example, medical imaging devices). Cyberattacks could also be directed toward medical devices that patients carry or wear, such as insulin pumps or pacemakers. Hence, a cyberattack on an AI-based medical device could impact the availability of healthcare systems, causing delays and disruptions in the provision of healthcare services. The unavailability of services may become fatal when patients' health conditions depend on such devices or require immediate hospitalisation.

Examples of such cyberattacks recently took place. For instance, during the WannaCry ransomware attack, thousands of appointments and operations were cancelled, and NHS

patients “had to travel further to accident and emergency departments.”¹ In Dusseldorf, a hospital targeted by ransomware redirected a woman suffering from an aortic aneurysm to another emergency department 32 km away. The distance delayed the patient’s treatment by one hour, and she died shortly after.²

Recent studies and medical device manufacturers’ disclosures highlighted the potential safety risks of these vulnerabilities, including those of AI-based medical devices.³ Those could include data poisoning, data exfiltration, or even social engineering.⁴

As will be visible from this article, the increase in cybersecurity risks for medical devices, exacerbated by the growing digitalisation of healthcare services in the US and the EU, has led legislators and regulatory bodies to pay more attention to the cybersecurity of medical devices. Artificial Intelligence policy documentation has been stressing the importance of cybersecurity throughout the years. Cybersecurity is essential for AI despite its lack of recognition in practice.⁵ The literature on medical device cybersecurity is growing, but it fails to study the governance of AI-based medical devices comprehensively. As of 2018, scholars have focused on selected problems related to AI and medical devices.⁶ In the EU, scholars have focused on medical devices and AI regulation about transparency or patients’ rights.⁷ In the US, scholars have studied the possible legal gaps in medical device cybersecurity laws, focusing on specific issues, such as critical infrastructure protection, best practices for medical device cybersecurity, security metrics for implantable medical devices, the cybersecurity of legacy medical devices, and liability.⁸

¹ National Audit Office, UK Department of Health, “Investigation: WannaCry Cyber Attack and the NHS” <<https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>> (last accessed 17 March 2024).

² W Ralston, “The Untold Story of a Cyberattack, a Hospital and a Dying Woman” (11 November 2020) <<https://www.wired.co.uk/article/ransomware-hospital-death-germany>> (last accessed 12 March 2024).

³ Food & Drug Administration, “Cybersecurity” [2023] FDA <<https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity>> (last accessed 12 March 2024).

⁴ E Biasin, E Kamenjasevic and KR Ludvigsen, “Cybersecurity of AI Medical Devices: Risks, Legislation, and Challenges” <<https://arxiv.org/abs/2303.03140>> (last accessed 30 November 2023); M Mozaffari-Kermani et al., “Systematic Poisoning Attacks on and Defenses for Machine Learning in Healthcare” (2015) 19 IEEE Journal of Biomedical and Health Informatics 1893.

⁵ Interestingly, from the very first EU policy documents preceding the AI Act proposal, the EU showed its concerns for AI-specific threats. See, for example, European Commission, “Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of Regions. Coordinated Plan on Artificial Intelligence” (2018) 8.

⁶ In the US, these have investigated the limits of FDA’s approaches towards SaMD and its new approach for AI/ML medical devices, see B Babic et al., “Algorithms on Regulatory Lockdown in Medicine” (2019) 366 Science 1202; B Boris et al., “Beware Explanations from AI in Health Care” (2021) 373 Science 284; J Boubker, “When Medical Devices Have a Mind of Their Own: The Challenges of Regulating Artificial Intelligence” (2021) 47 American Journal of Law & Medicine 427.

⁷ Some other authors in the EU concentrate their analysis on the interplay between medical devices, AI and cybersecurity regulations in the EU – with seemingly no counterpart in the US.

⁸ See L Hagen, “Coding for Health: Cybersecurity in Medical Devices” (2016) 28 Health Lawyer; C Kersbergen, “Patient Safety Should Include Patient Privacy: The Shortcomings of the FDA’s Recent Draft Guidance Regarding Cybersecurity of Medical Devices” (2017) 41 Nova Law Review 397; CA Tschider, “Enhancing Cybersecurity for the Digital Health Marketplace” (2017) 26 Annual Health Law 1. T Check, “The Tallinn Manual 2.0 on Nation-State Cyber Operations Affecting Critical Infrastructure” (2023) 13 American University National Security Law Brief; SJ Shackelford et al., “Securing the Internet of Healthcare” (2018) 19 Minnesota Journal of Law, Science and Technology 405; C Camara, P Peris-Lopez and JE Tapiador, “Security and Privacy Issues in Implantable Medical Devices: A Comprehensive Survey” (2015) 55 Journal of Biomedical Informatics 272; R Lord and D Roseen, “Do No Harm 2.0”; KB Wellington, “Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions” (2014) 30 Santa Clara High Technology Law Journal 139; L Dudin, “Networked Medical Devices: Finding a Legislative Solution to Guide Healthcare into the Future” (2017) 40 Seattle University Law Review 1085; BA Corbin, “When ‘Things’ Go Wrong: Redefining Liability for the Internet of Medical Things” (2019) 71 South Carolina Law Review 1.

There have been studies comparing the EU and the US.⁹ Nevertheless, all these studies have fallen short in assessing AI and cybersecurity unitedly for medical devices.¹⁰

2. Methodology

The EU and the US regulatory systems for AI-based medical device cybersecurity are evolving. In such an evolution of regulatory fields, knowing what other regulators are doing in terms of rules may help think about the current and future regulatory approaches. This article, therefore, aims to analyse and compare the current EU legal systems on medical devices with the US, applying a prospective focus on what the future AI and cybersecurity regulations could entail for them.

The article considers Kestemont's legal methodology and adopts its "external comparative approach."¹¹ It studies the EU/US legal systems, their laws and regulations concerning medical devices, their regulatory oversight mechanisms, and the possible changes that could be entailed following AI and cybersecurity legislation. We assume a macro-comparative law perspective considering the legal system's structure of medical device laws, assessed against two new elements currently legislated and affecting them – AI and cybersecurity.

The paper is structured as follows. We first summarise the main aspects of the EU and US legal systems on medical devices and the rules that may be pertinent to them concerning AI and cybersecurity. Secondly, for each legal system, we describe the regulatory approaches towards AI and cybersecurity and their application for medical devices. In the central part of the paper, we highlight the core differences in regulations and offer macro-comparative insights. We conclude that the two regulatory systems have notable differences and that some aspects of each system could be helpful for the other.

II. Analysis

I. The legal framework on medical devices of the European Union

The legal framework applicable for AI-based medical devices is composed of a set of laws that intertwine with one another.¹² The primary legislation concerning medical devices is the Medical Device Regulation (MDR) and the In Vitro Device Regulation (IVDR). The MDR and the IVDR recently entered into force after the reform of the EU medical device legal framework, established in the 1990s in the wake of the so-called New Approach

⁹ For comparative studies see S Lyapustina and K Armstrong, "Regulatory Considerations for Cybersecurity and Data Privacy in Digital Health and Medical Applications and Products" (2018) Inhalation; I Skierka, "The Governance of Safety and Security Risks in Connected Healthcare," *Living in the Internet of Things: Cybersecurity of the IoT - 2018* (Institution of Engineering and Technology 2018) <<https://digital-library.theiet.org/content/conferences/10.1049/cp.2018.0002>> (last accessed 17 March 2024); Y-J Chen et al., "A Comparative Study of Medical Device Regulations: US, Europe, Canada, and Taiwan" (2018) 52 Therapeutic Innovation & Regulatory Science 62.

¹⁰ There is little literature concerning AI-based medical device cybersecurity at this point in time. See C Tschider, "Medical Device Artificial Intelligence: The New Tort Frontier" (2021) 46 Brigham Young University Law Review 1551.

¹¹ L Kestemont, *Handbook on Legal Methodology: From Objective to Method* (Intersentia 2018) 46–50 <<https://www.cambridge.org/core/books/handbook-on-legal-methodology/B957C53FFA068812AB435BD51890EDEC>>. More specifically, we consider its "functional approach," which takes the broader context of the legal systems, including legislative proposals for comparison.

¹² We already described elsewhere the current and forthcoming legal framework for AI-based medical devices. See E Biasin, B Yašar and E Kamenjašević, "New Cybersecurity Requirements for Medical Devices in the EU: The Forthcoming European Health Data Space, Data Act, and Artificial Intelligence Act" (2023) 5 Law, Technology and Humans 43.

wave.¹³ The MDR/IVDR are EU regulations, meaning that they directly apply in the EU Member States. The legislation follows a risk-based approach, meaning that medical devices can be marketed across the European Union depending on the risks they pose to the health and safety of users and patients. There exist cybersecurity-related obligations in the MDR and IVDR, which are present in the form of “safety and performance” requirements, and which are contained in the Regulation’s annexes.¹⁴ For example, Annex I of the MDR requires that medical devices be designed and manufactured to suit their intended purpose and that they be safe and effective. Manufacturers must adhere to state-of-the-art development principles, including risk management, verification, validation and specific IT security measures.¹⁵

EU legislation that entail consequences for medical devices are also present in other cybersecurity and AI laws. The NIS2 Directive and the Cybersecurity Act are the most relevant to report for cybersecurity laws. The NIS2 Directive applies to medical device manufacturers and sets cybersecurity risk management and incident notification requirements.¹⁶ The Cybersecurity Act establishes voluntary certification mechanisms applicable to medical devices.¹⁷ The forthcoming AI legislation is also deemed to apply to medical devices. The essential reference in this regard is the draft AI Act. The draft AI Act may apply to medical devices, and it includes cybersecurity-related requirements applicable to them.¹⁸

2. The legal framework on medical devices in the United States

The current legal framework for medical device cybersecurity comprises different pieces of legislation.¹⁹ In the US, the primary legislation to consider for medical devices is the Food, Drug, and Cosmetics Act (FD&C Act), which sets the main requirements concerning medical devices. Interestingly, the act explicitly refers to cybersecurity and foresees specific requirements under section §360n-2 titled “Ensuring cybersecurity of devices.”

¹³ The New Approach was developed in 1985 in the European Union. It was proposing to regulate in legal acts only the main rules, ie “the essential requirements,” while leaving the more specific details of legislation to European harmonised standards. The New Approach differs from the “Old Approach,” where legal texts were detailing all the technical and administrative requirements. EU policymakers established the New Approach to allow a more flexible legislation to address to the rapid evolution of products and technologies.

¹⁴ These cybersecurity-related obligations were interpreted in 2019 by the Medical Device Coordination Group (MDCG). The MDCG is an entity established by the MDR, which has the task – among others – to issue guidelines on the interpretation of the MDR itself. In its the Guidelines on cybersecurity of medical devices, the MDCG analysed the MDR/IVDR from a safety and security perspective.

¹⁵ MDR, Annex I, req 4, 14, 17.

¹⁶ For an analysis of the NIS2 and Cybersecurity Act in detail, see E Biasin and E Kamenjašević, “Cybersecurity of Medical Devices: New Challenges Arising from the AI Act and NIS 2 Directive Proposals” (2022) International Cybersecurity Law Review <<https://doi.org/10.1365/s43439-022-00054-x>>. It is worth noting that the current NIS Directive is indirectly relevant to medical device cybersecurity, too. See E Biasin and E Kamenjasevic, “Cybersecurity of Medical Devices: Regulatory Challenges in the European Union” in C Shachar et al. (eds), *The Future of Medical Device Regulation: Innovation and Protection* (Cambridge University Press 2022) <<https://www.cambridge.org/core/books/future-of-medical-device-regulation/cybersecurity-of-medical-devices/AC01289C2DB05E44D0D98A9E66666562>>.

¹⁷ While this regulation sets the procedure for any type of certification scheme, it is important to note that, at the moment, no scheme has been adopted for medical devices. See also *Ibid.* for an analysis of how the Cybersecurity Act is relevant to medical devices.

¹⁸ Notably, Article 15 establishes cybersecurity requirements for high-risk AI systems and establishes a presumption of conformity for medical devices that are certified based on the Cybersecurity Act. For a broader discussion about the application of the draft AI Act to medical devices, see S Palmieri and T 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.

¹⁹ For reasons of scope and space, our analysis focuses only on federal-level legislation.

Similar to the EU, in the US, other pieces of legislation apply in parallel to medical devices and establish further requirements in the field of AI and cybersecurity. The most relevant reference for the US cybersecurity law is the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which foresees incident reporting and other requirements applicable to medical devices.²⁰ In addition to the CIRCIA, it is noteworthy to report the statute signed by the US president in December 2022, which has impacted the regulation of medical device cybersecurity and AI with further requirements and provided authority to the FDA to establish cybersecurity standards for medical devices.²¹

Until today, the US has not adopted any comprehensive piece of legislation governing AI. There have been specific AI governance initiatives, including executive orders and specific proposed acts and bills.²² The latest development of the US AI policy occurred on 30 October 2023, when the president of the United States issued an executive order on the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence. The executive order includes eight main guiding principles with a strong emphasis – among others – on safety, security, privacy and confidentiality. The exact order entails the US Department of Health and Human Services (HSS) to develop a strategic plan including policies and frameworks concerning AI-based health technologies.²³

3. Soft law in the EU and US

Guidance documentation non-binding recommendations (also called “soft law”) play an essential role in medical device regulation in the EU and the US. In the US and EU, health regulatory authorities interpret medical device regulations and may issue guidance documentation.

The EU has had a long-standing guidance portfolio, formerly by MEDDEV and now by the MDCG.²⁴ The first EU-level guidance on medical device cybersecurity was issued in 2019.²⁵ In the US, the FDA has published guidance on medical device cybersecurity since 2005. It is also worth noting that the EU and the US are part of the International Medical Devices Regulatory Forum (IMDRF). The IMDRF is a voluntary group of medical device regulators that have agreed to collaborate to accelerate international medical device regulatory convergence. The IMDRF has also issued documentation guidance,

²⁰ These foresee incident reporting and other requirements soon to be specified by forthcoming comprehensive guidelines on reporting.

²¹ US, Consolidated Appropriations Act, 2023, section 3305 and subs.

²² See for example, President of the United States, Executive Order “Maintaining American Leadership in Artificial Intelligence” (2019); President of the U.S. Executive Order “Promoting the Use of Trustworthy AI in the Federal Government” (2020); the draft Algorithmic Accountability Act of 2022, among others. For a discussion of the US legislative approach on AI, see K Vranckaert, “How Cautious Is Too Cautious? The US and EU Artificial Intelligence Roadmap (Part 3: The Algorithmic Accountability Act 2022)” (*CiTIP blog*, 16 May 2023) <<https://www.law.kuleuven.be/citip/blog/how-cautious-is-too-cautious-the-us-and-eu-artificial-intelligence-roadmap-part-3-the-algorithmic-accountability-act-2022/>> (last accessed 12 March 2024).

²³ President of the United States, Executive Order “Safe, Secure and Trustworthy Development and Use of Artificial Intelligence” (30 October 2023), sec 8.

²⁴ Before the MDCG, MEDDEV was the entity that was tasked to provide guidance and suggest a common approach for manufacturers and notified bodies involved in conformity assessment procedures.

²⁵ Medical Device Coordination Group, “MDCG 2019-16 Guidance on Cybersecurity for Medical Devices” (2019) <https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf>. According to certain authors, the guidance is in need of revisions. See D Milojevic, “Is It Time to Update the Medical Device Coordination Group’s Guidance on Cybersecurity for Medical Devices? – CiTiP Blog” (*KU Leuven CiTiP Blog*, 14 November 2023) <<https://www.law.kuleuven.be/citip/blog/is-it-time-to-update-the-medical-device-coordination-groups-guidance-on-cybersecurity-for-medical-devices/>> (last accessed 12 March 2024).

which is non-binding for medical device manufacturers, representing a point of reference in terms of best practices for medical device stakeholders. The IMDRF has published principles and practices in cybersecurity, legacy medical devices, and software bills of materials.²⁶

III. The governance of AI and cybersecurity for medical devices: two systems into comparison

The governance framework for AI and cybersecurity of medical devices is shifting rapidly as policy initiatives evolve in the EU and the US. As the respective legal systems evolve, tracing parallels and comparing the differences in approaches is helpful. With this objective in mind, the subsequent sections comment on three main aspects: legislation, regulatory guidance by competent health authorities, and regulatory oversight. The main findings are summarised in the table below (Table 1):

I. Preliminary comparisons: the EU principle-based vs the US rule-based systems

Before delving into the specificities of AI and cybersecurity regulation for medical devices, it is worth observing the main differences between the two systems. Scholars in medical device studies have proposed two classifications for the EU and the US systems: command-and-control/rule-based regulations versus principle-based regulations.²⁷ The US belongs to the “rule-based system.” This system’s characteristic consists of the regulator setting specific and precise rules that the regulated entities (manufacturers) must follow. In this regulatory model, the regulator (ie the FDA) has the power to create and detail the applicable rules for medical devices through regulatory guidance, which are issued continuously as they have to adapt to technological developments.²⁸ The EU belongs to the “principle-based” system. The principle-based approach is different. It is based on adopting broad principles (rather than specific rules) and foreseeing fundamental obligations (ie MDR/IVDR safety requirements) that parties should all observe.²⁹ Its principles are encompassing, and their specification is delegated to harmonised standards.³⁰

These preliminary differentiations may look theoretical. However, they help understand the differences in the regulatory approaches in the EU and US for medical device cybersecurity. As it will also be seen further, they may explain why the FDA has produced more guidance for novel matters such as cybersecurity and AI compared to the EU. The explanation relies on the fact that, structurally, the FDA is called more often to provide specific rules as part of the rule-based system, whereas, in the EU, the problem of having specific rules on novel technologies becomes less urgent given the flexibility provided by the general principles of safety requirements.

²⁶ International Medical Device Regulators Forum, “Principles and Practices for Medical Device Cybersecurity” (2020); International Medical Device Regulators Forum, “Principles and Practices for the Cybersecurity of Legacy Medical Devices”; International Medical Device Regulators Forum, “Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity” (2023).

²⁷ A Wilkinson, “Medical Device Regulation and Litigation: A Comparative Analysis of Australia, the United Kingdom and the United States of America” (PhD, Queensland University of Technology 2021) <<https://eprints.qut.edu.au/209677>> (last accessed 12 March 2024).

²⁸ Based on the competences provided by the law.

²⁹ J Black, M Hopper and C Band, “Making a Success of Principles-Based Regulation” (2007) 1 Law and Financial Markets Review 191, 194.

³⁰ In the past the association was more evident, as it relied to the so-called “essential requirements.”

Table I. Governance of AI and cybersecurity for medical devices (US/EU)

	US rule-based system	EU principle-based system
Legislation	Medical Devices: FDC&A. Cybersecurity: CIRCIA. AI: no federal horizontal AI laws. Presence of state-specific laws with an impact on AI. *Other laws, eg data protection and non-discrimination laws.	Medical Devices: MDR/IVDR. Cybersecurity: NIS Directive, Cybersecurity Act. AI: (draft) AI Act, national-specific laws with an impact on AI. *Other laws, eg data protection and non-discrimination laws.
Soft-law	Guidance on AI-based Medical Device Cybersecurity FDA Cybersecurity guidance ("may apply to AI-based medical devices"). FDA AI/ML Good practices (refer to cybersecurity).	Guidance on Medical Device Cybersecurity MDCG: Cybersecurity guidance (no reference to AI). MDCG: no AI-specific guidance.
Regulatory oversight	FDA-centralised approval and oversight *Definition of medical device: narrow. * Regulatory pathway: based on class risks. Pre-market, 510(k), de novo.	Third-party approval and national health authority oversight *Definition of medical devices: narrow. *Regulatory pathway: based on class risks. Self-assessment or third-party assessment.

2. On legislation: comparative remarks

Let us now turn to the comparative analysis of medical device legislation, with an eye on AI and cybersecurity initiative that may impact it. The first element we analyse is the current state of the art for the applicable laws on AI and cybersecurity for medical devices.

As a first point, we assess whether AI or cybersecurity are mentioned in the EU and US medical device laws. In the EU, the MDR/IVDR do not mention specifically "cybersecurity" or "AI."³¹ However, their relevance can be inferred from the rules on "software" and the interpretation of the "safety and performance" requirements. In the US, similarly, the FD&C Act does not explicitly mention "artificial intelligence" while it does mention explicitly "cybersecurity."³²

As a second point, we assess the regulatory state of the art of AI laws impacting AI-based medical device cybersecurity. As seen above, the EU is approving a horizontal legislation that will apply to medical devices.³³ This legislation will also include cybersecurity-related provisions under Article 15, which may apply to medical devices when considered high-risk AI systems. Currently, the US does not have comprehensive federal legislation on AI. The most recent initiative is the October 2023 executive order, which details several directives for federal agencies and a strategic plan that could include policies and frameworks on responsible deployment and use of AI and AI-enabled technologies in the health and human services sector.³⁴ According to the same executive order, these should include safety, privacy and security standards in software development and take due account of AI-enhanced cybersecurity threats. Beyond the executive order, national (draft)

³¹ This approach might be also possibly explained for the MDR/IVDR to pursue the objective of technology neutrality.

³² See section §360n-2 titled "Ensuring cybersecurity of devices," which includes cybersecurity related requirements.

³³ The application to medical devices has some caveats. The critical aspects of the AI Act application to medical devices are detailed by Palmieri and Goffin (n 18).

³⁴ President of the United States, Executive Order "Safe, Secure and Trustworthy Development and Use of Artificial Intelligence" (30 October 2023), sec 8.

laws exist that touch upon certain AI aspects in healthcare but are of minor relevance to cybersecurity.³⁵

The third point concerns cybersecurity requirements set by cybersecurity legislation and applicable to medical devices. In addition to the MDR/IVDR safety requirements (which we explained to have cybersecurity-related provisions), there are two applicable laws in the EU: the NIS2 Directive and the Cybersecurity Act. In the US, the CIRCIA that envisages incident notification requirements which may apply to medical devices. In this case, the EU/US situation presents several similarities, which may be summarised by the fact that both systems foresee cybersecurity legislation providing for incident notification requirements.³⁶

Based on the above, we observe that the US and EU are in different legislative situations. Both the EU and the US have medical device legislation. They also have horizontal cybersecurity legislation. The two systems differ, however, in the regulation of AI. While the EU is adopting a hard-law horizontal approach to AI regulation, the US seems not to be headed adopting (at this moment) to federal wide-reaching legislation applying horizontally to AI systems. The new executive order has delegated HSS to issue guidance on sector-specific matters, therefore, many aspects of AI governance will likely be delegated to the regulatory authorities or federal entities.

3. On regulatory guidance: comparative remarks

This section analyses in a comparative perspective how and to what extent the regulatory authorities have addressed AI and cybersecurity in their guidance on medical devices.

As seen above, the relevant entities in the EU and the US have issued guidance related to medical devices. For cybersecurity, The EU issued its first EU-level guidance on medical device cybersecurity in 2019.³⁷ The guidance explains the safety requirements relevant to cybersecurity as applied to medical devices. Before this guidance, there was no EU-wide cybersecurity guidance documentation specific to medical devices. In the US, the FDA has produced guidance documentation on cybersecurity since 2005. In fact, 2005 was the year when the FDA started producing a set of principles in its guidance on Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software. In 2014 and 2016, the FDA issued its Guidance for Pre-market Submission and Post-market Management of Cybersecurity in Medical Devices, one of which was recently renewed in September 2023.³⁸ Turning to AI-related guidance, the EU has not explicitly produced (yet) any piece of guidance on medical devices primarily addressing AI. The scenario is different for the US, where the FDA has been issuing relevant documentation as of 2019.³⁹ In April 2021, the FDA released its Artificial Intelligence and Machine Learning (AI/ML) Software as a Medical Device Action Plan in response to its 2019 reflection paper on the same matter.⁴⁰ Further,

³⁵ For a detailed overview, see “The State of State AI Laws: 2023” (EPIC – Electronic Privacy Information Center, 3 August 2023) <<https://epic.org/the-state-of-state-ai-laws-2023/>> (last accessed 12 March 2024).

³⁶ The paragraph here considers only cybersecurity laws for the sake of simplicity. Incident notification is not only a cybersecurity law prerogative. For a broader discussion on how medical device laws may have incident notification rules from a cybersecurity perspective, see Biasin and Kamenjasevic (n 16).

³⁷ Medical Device Coordination Group (n 25).

³⁸ Food & Drug Administration, “Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software”; Food & Drug Administration, “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices” (2014); Food & Drug Administration, “Postmarket Management of Cybersecurity in Medical Devices” (2016). The 2014 guidance was recently reviewed, see Food & Drug Administration, “Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions” (2023).

³⁹ Food & Drug Administration, “Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD)”.

⁴⁰ Food & Drug Administration, “Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan” (2021); Food & Drug Administration, “Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD)” (n 39).

in 2021, the FDA released its Good Machine Learning Practices for Medical Devices Development, where it mentioned “robust cybersecurity practices” as part of the guiding principle of “Good Software Engineering and Security Practices.”⁴¹

The comparison between the US FDA and the EU MDCG shows the different situations where the two regulatory authorities stand. The US FDA has provided more (and for much longer) documentation guidance about medical device cybersecurity, AI-based medical devices and the intersection between the two elements. The EU MDCG has started only recently, and – as some authors argue – the only guidance about cybersecurity already needs to be updated.⁴² The different approach can be explained by the fact that the US system, which is rule-based, gives much more power and leeway to the FDA to set specific rules for medical devices.⁴³ Differently, the EU, which has a principle-based system, has more flexible requirements that delegate interpretation and best practices to adhere to technical standards.

4. On regulatory oversight: comparative remarks

The third element that this paper discusses concerns the regulatory oversight of medical devices, in general, and when it comes to AI-enhanced cybersecurity. This third element may show the most significant difference between the US and the EU regulatory system. In the US, the FDA retains regulatory oversight for approving and monitoring manufacturer’s compliance with medical device rules and regulations. This kind of oversight is centralised and it depends on the competence and powers historically attributed to federal authorities in the US.⁴⁴ The situation in the EU is different. Conformity assessment and approval of medical devices is delegated to notified bodies identified and delegated by national health authorities. There is no centralised authority in the EU that oversees medical devices’ compliance with MDR/IVDR laws.⁴⁵

Regulatory pathways are also different.⁴⁶ As Muehlmatter et al. show, there is no specific pathway for AI/ML-based medical devices in the EU and US.⁴⁷ In both cases, the medical device must undergo a standard evaluation process. The EU has one main risk-based procedure, distinguishing between risk classes. The US also differentiates based on medical device classes. However, the US provides for an additional and specific procedure that finds no correspondence in the EU, the so-called “510(k) pathway.” The 510(k) pathway – which may apply to class I, II and III medical devices for which pre-market approval is not indicated – allows the evaluation procedure to be based on the comparison

⁴¹ Food & Drug Administration, Health Canada and Medicines and Healthcare products Regulatory Agency, “Good Machine Learning Practice for Medical Device Development: Guiding Principles” (2021).

⁴² Milojevic (n 25).

⁴³ To this, it should be added that all MDCG acts are non-binding, while FDA’s guidance in certain contexts are. See Food & Drug Administration, “What Is the Difference between the Federal Food, Drug, and Cosmetic Act (FD&C Act), FDA Regulations, and FDA Guidance?” (FDA, 28 June 2021) <<https://www.fda.gov/about-fda/fda-basics/what-difference-between-federal-food-drug-and-cosmetic-act-fdc-act-fda-regulations-and-fda-guidance>> (last accessed 12 March 2024).

⁴⁴ Majone explains why EU and US authorities are different in terms of competence and powers. See G Majone, “The New European Agencies: Regulation by Information” (1997) 4 Journal of European Public Policy 262.

⁴⁵ The reasons behind this factual situation is historical. At the moment of first establishing of medical device laws, the EU could not delegate such a task to a European health authority, due to the division of competences in the matter of health law. On this point, see A Wilkinson, “Medical Device Regulation and Litigation: A Comparative Analysis of Australia, the United Kingdom and the United States of America” (PhD, Queensland University of Technology 2021) <<https://eprints.qut.edu.au/209677>> (last accessed 12 March 2024, 251).

⁴⁶ For a comparative analysis, see UJ Muehlmatter, P Daniore and KN Vokinger, “Approval of Artificial Intelligence and Machine Learning-Based Medical Devices in the USA and Europe (2015–20): A Comparative Analysis” (2021) 3 The Lancet Digital Health e195.

⁴⁷ Ibid.

of a device to one or more similar legally marketed devices (predicate device). Although the 510(k) procedure is deemed to incentivise innovation, it has been criticised for concerns over safety by several healthcare stakeholders throughout the years.⁴⁸ For AI-based medical device cybersecurity, this procedure could become problematic. As the safety and security of former devices are likely to have different and lower cybersecurity standards, this may lower security standards for AI-based medical devices. Finally, a topic connected to the issue of authority oversight concerns the scope and application of medical device regulations. It is worth reporting discussions about the EU/US definition of medical device software in the literature. Many scholars in the EU and US academia seem to agree that, for AI-based medical devices, the existing definitions are narrow and exclude specific possibly risky devices.⁴⁹

In light of the above comparison, it is clear that the EU and the US have different settings concerning regulatory approval and oversight of medical devices. The US has a centralised federal system, while the EU has a decentralised and delegated system for approval and oversight. In terms of procedures, we observed that the US foresees a regulatory pathway that has no correspondence with the EU, whose (already debated) safety concerns may also have consequences for AI-based medical device cybersecurity.

IV. Conclusion

This paper analysed the EU and US legislative and regulatory approaches concerning AI and cybersecurity for medical devices. Our analysis showed that the field focusing on AI-based medical device cybersecurity specifically is relatively new and in the process of being established, both in the US and the EU.

AI and cybersecurity laws applicable to medical devices are being made in the EU and the US. We noted that the US has a longer tradition of regulating medical devices and cybersecurity. On the contrary, the EU has more recent legislation on medical devices but is now establishing and preceding the US in setting hard laws regulating artificial intelligence.

On regulatory activities, we observed that the US has been at the forefront of AI and cybersecurity for medical devices. The EU has been lagging behind cybersecurity guidance – as it issued more than ten years later – and AI, which is still nonexistent at the time of writing. We hypothesised that this difference in regulatory guidance provision depends on the US belonging to the rule-based regulatory system, requiring regulatory authorities to frequently issue specific rules, whereas, in contrast, the EU belongs to the principle-based system, which allows for a more flexible interpretation of the MDR/IVDR safety and performance requirements.

Finally, we highlighted the significant differences in regulatory oversight between the EU and the US. We noted that the US has a rather centralised system for approval and oversight, while the EU relies on a third-party and territorial system. This system makes it more likely for US authorities to have a firmer grip on overseeing medical devices' safety requirements since they can monitor them continuously and throughout their lifecycle.

⁴⁸ For an overview of the 510(k) procedure safety issues, see AW Collins, "The FDA's 510(k) Approval Process and the Safety of Medical Devices" (Temple University 2023) <<https://www.proquest.com/openview/0e095991c7b9f8140dd20b0aa62cdcd4/1?pq-origsite=gscholar&cbl=18750&diss=y>>.

⁴⁹ In the US, Gerke argued that the definition of the term medical device is too narrow and excludes several risky AI-based health products. These are, for example, Clinical Decision Support Software (CDS), AI-based mortality prediction models, and other models that are intended for use in the prediction or prognosis of diseases or other conditions. See S Gerke, "Health AI for Good Rather Than Evil? The Need for a New Regulatory Framework for AI-Based Medical Devices" (2021) 20 Yale Journal of Health Policy, Law, and Ethics 511. In the EU, Palmieri and Goffin observe that the draft AI Act is a "blanket that leaves the feet cold" for certain AI-based medical devices, meaning that certain low-risk devices are excluded from the scope. See Palmieri and Goffin (n 18).

This grip might be less effective in the EU, as it relies on a third-party notification system assessment while leaving the post-market checks to the Member States' regulatory authorities. We also highlighted the differences in the regulatory pathway, where the US 510(k) predicate system may open more safety concerns for AI-enhanced cybersecurity.

Finally, we also noted that literature on AI-based medical device cybersecurity is flourishing but relatively scarce. Future research should address AI-based medical device cybersecurity, in general, in its meaning across the product lifecycle and its relationship with horizontal cybersecurity and AI laws.

Acknowledgments. This manuscript summarises the findings of the research project “Transatlantic Perspectives on AI-Based Medical Device Cybersecurity” that we conducted in 2022–2023 within the Stanford Law School–University of Vienna Transatlantic Technology Law Forum (TTLF). We are grateful to Prof. Siegfried Fina, Prof. Roland Vogl, and Prof. Mark Lemley for the research opportunity. We are indebted to Prof. Federica Casarosa and Dr. Jaroslaw Greser for their interest in our research, for the insightful discussions at the European University Institute, and the comments to earlier versions of the manuscript. All errors are our own.