


ARTICLE

# The Regulatory Environment for the Safety of the Internet of Medical Devices Users in the European Union and the United States

Katarzyna Biczysko-Pudełko 

Faculty of Law and Administration, University of Opole, Opole, Poland

Email: [kbiczysko@uni.opole.pl](mailto:kbiczysko@uni.opole.pl)

## Abstract

The Internet of Medical Things (IoMT) devices, as well as the Internet of Things phenomenon itself, are gaining a new group of customers every day, for whom it is almost a matter of course to use a wide range of devices, such as Internet-connected complex life support equipment or “smart” watches monitoring basic life parameters. With the growing popularity of such devices, however, questions about the safety of their users begin to arise, because almost in proportion to the number of benefits associated with the use of these products, the number of risks associated with them increases – eg improper functioning of Internet-connected life support equipment, in addition to threatening the life or health of its user, may affect the physical security of the product itself, the security of both personal and technical (eg non-personal) data processed by the specific product, or finally the cyber-security of the product. While the issues related to the protection of personal data and privacy, in general, have been discussed many times by the doctrine, the issues related to the protection of users of these devices under consumer law have not been considered much.

In this context, the question arises whether the current legal regulations provide an adequate and sufficient level of protection for IoMT users. In particular, whether the average IoMT user can actually exercise their rights under the provisions of consumer law and whether the protection afforded to him – both in terms of the scope of their rights and the scope of obligations and liability of manufacturers and suppliers of these devices – is not only illusory? In order to answer the above questions, the author will evaluate the prevailing market practices – still focused around the doctrine of “caveat emptor” or “let the buyer beware” – and compare them with these regulations and juxtapose them with relevant legal regulations. However, given the lack of geographical borders in the field of cyber security and privacy, the author will not only analyse EU cyber security legislation, but also US legislation in a comparative legal analysis. The choice of jurisdictions to be compared is also related to the size and importance of both the US and the EU for the global IoMT market. It should be noted that the United States has a dominant position in the IoMT, while the European Union is estimated to have the second largest IoMT market globally. At the same time, however, there are differences in legal systems between the two economic areas. An analysis carried out in this way will make it possible not only to answer the question posed above, but also to possibly identify those areas of regulation that need to be changed or adapted to the realities of IoMT.

**Keywords:** consumer; European Union law; Internet of Medical Things (IoMT); United States law

## I. Introduction

There is no doubt that the Internet of Things<sup>1</sup> (within which, to put it very graphically, thing-to-thing communication takes place<sup>2</sup>) is shaping our reality more boldly every year and will influence it even more shortly. This is evidenced by statistics according to which, in the world, the number of devices connected reached 11.7 billion in 2020, while – it is estimated – by 2025 there will be more than 64 billion IoT devices.<sup>3</sup> This state of affairs is certainly a consequence of the range of benefits that the use of this technology brings – ie making everyday activities easier, saving time, etc. Moreover, IoT is even seen by some as “a revolutionary, fully connected ‘smart’ world of progress, productivity, and opportunity, with the potential to add billions of value to industry and the global economy”.<sup>4</sup>

The above trend also applies to the so-called Internet of Medical Things (IoMT), where the market for connected medical devices is estimated to reach USD 36.1 billion worldwide by 2023, with a growth rate of 21.1%<sup>5</sup> between 2018 and 2023 – which is not surprising if one considers the benefits it can bring both to individual patients or users and to medical staff or medical facilities – ie reducing healthcare costs, providing timely medical care and increasing the quality of treatment.<sup>6</sup>

However, like any technology, the use of IoMT may bring a number of legal and non-legal challenges, which impose on legislators the obligation to create a regulatory environment protecting users as adequately as possible. The subject of this analysis will be an attempt to describe the regulatory environment in the European Union and the United States and to answer the question: Do the current legal regulations provide an adequate and sufficient level of protection for IoMT user-consumers? This research question directly determines the structure of the work. After a brief introduction to the concept and classification of IoMT, the analysis is divided into two main parts dedicated, respectively, to European and US legislation, addressing in detail the issue and the concept of “medical devices.” It should be emphasised that the aim of this paper is not a traditional comparative legal analysis of the two legal orders and a case-by-case comparison of individual legal provisions, but only a kind of synthetic illustration of the position of the users of these IoMT devices and their level of safety.<sup>7</sup>

## II. Definition and classification of the internet of medical things

IoMT are medical devices able to communicate, collect and exchange data via WiFi networks and online platforms. These devices can provide up-to-date patient information,

<sup>1</sup> Hereinafter IoT.

<sup>2</sup> L. Tan, N. Wang, “Future Internet: The Internet of Things” in 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE) (2010).

<sup>3</sup> Christo Pietrow, “26 Stunning Internet of Things Statistics 2022 (The Rise Of IoT)” <<https://techjury.net/blog/internet-of-things-statistics/#gref>> (last accessed 12 November 2023).

<sup>4</sup> Vivek Singhania, “The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected orld” (2016) <[https://www.academia.edu/28441059/The\\_Internet\\_of\\_Things\\_An\\_Overview\\_Understanding\\_the\\_Issues\\_and\\_Challenges\\_of\\_a\\_More\\_Connected\\_World](https://www.academia.edu/28441059/The_Internet_of_Things_An_Overview_Understanding_the_Issues_and_Challenges_of_a_More_Connected_World)> (last accessed 12 November 2023).

<sup>5</sup> Mohammed Khan, “The Internet of Medical Things—Anticipating the Risk” (2019) <<https://www.isaca.org/resources/isaca-journal/issues/2019/volume-4/the-internet-of-medical-things-anticipating-the-risk>> (last accessed 12 November 2023).

<sup>6</sup> Mohan Krishna Kagita, Navod Thilakarathne, Thippa Reddy Gadekallu, Praveen Kumar Reddy Maddikunta, “A Review on Security and Privacy of Internet of Medical Things” in Uttam Ghosh, Chinmay Chakraborty, Lalit Garg, Gautam Srivastava (eds) *Intelligent Internet of Things for Healthcare and Industry. Internet of Things*. (Springer 2022), 171.

<sup>7</sup> For a comparison of the EU and US legal system as regards the interplay between medical regulation, cybersecurity and artificial intelligence, see Elisabetta Biasin, Erik Kamenjašević, *Regulatory Approaches Towards AI-Based Medical Device Cybersecurity: an EU/US Transatlantic Perspective*, forthcoming.

increase patient self-sufficiency and reduce the cost of care.<sup>8</sup> However, such general definition encompasses a range of devices that can be classified into different subcategories, namely:

- (1) Implantable devices – these are typically devices designed for long-term use such as cochlear implants, pacemakers and insulin pumps. The possibility of their use depends on a prior decision of the physician in this regard, and the process of their activation is carried out as part of a specific medical procedure;
- (2) Clinical-grade fixed medical devices – these are part of the equipment of hospitals or medical facilities, where they are used for administrative or clinical functions. Importantly, although these devices are located in medical facilities, their users employ them remotely. This category includes, for example, infusion pumps or other devices that monitor patients' vital signs;
- (3) Stationary “in-home” medical devices – devices which are located in the patient's home and serve the purpose of remote monitoring of the patient's health condition and basic physiological parameters by medical personnel, eg in order to support long-term care in the patient's home;
- (4) “Wearable” devices – these are “consumer” devices whose main purpose is to monitor the basic physiological parameters of their users and collect data presented directly to the user – ie common smart watches that monitor pulse or sleep quality, which can be verified by the user at any time. Such devices can be purchased by the user individually, for their own purposes, without the need to consult a doctor.<sup>9</sup>

Obviously, the division presented earlier is not exhaustive and many different concepts as to the qualification of IoMT devices can be found in the literature.<sup>10</sup> From the point of view of the present analysis, however, it seems important to draw attention to the fact that some of these devices are of a strictly “consumer” nature, ie intended mainly for personal use (such as smart watches), while others have a clinical purpose. This leads directly to the question of whether such distinction will affect the scope of protection for users of these devices and, if so, whether, in relation to both “consumer” IoMT devices and clinical devices, the protection afforded by the law will be adequate and sufficient?

The author will, however, seek an answer to this question only in relation to the cyber and physical security of these devices – although it should be pointed out that the concept of security as such will also include such subcategories as the security of the product itself<sup>11</sup> or the security of the data processed.<sup>12</sup> Cybersecurity should be understood as the appropriate level of a product's performance and the fact that it is equipped with tools and mechanisms to counter ICT threats. Physical security, on the other hand, will refer to the impact of technology and its application on the physical world, ie the direct impact and influence of the IoMT world on users' daily lives and health.

<sup>8</sup> Bethany A. Corbin, “When ‘Things’ Go Wrong: Redefining Liability for the Internet of Medical Things” (2019) 71 South Carolina Law Review 1, 1.

<sup>9</sup> These devices may be defined also as “mixed functions” devices, see Francesca Gennari, Standards and Liability: What About Mixed Functions IoT devices?, forthcoming.

<sup>10</sup> See more: “Internet of Medical Things Revolutionizing Healthcare” <<https://aabme.asme.org/posts/internet-of-medical-things-revolutionizing-healthcare>> (last accessed 12 November 2023); Khan, (n 5).

<sup>11</sup> In this respect, product safety should be identified from the point of view of standards relating to hygiene, toxicity, functionality, ergonomics, etc., which guarantee the safe use of the product.

<sup>12</sup> Data cyber security will be related to the processing by a product, or ecosystem, of ambient information, both personal and technical (eg non-personal).

### III. The regulatory environment in the European Union

No single legal act in the European Union regulates IoMT issues comprehensively and horizontally. The regulatory environment is shaped by several different types of vertical legal acts, which have a different scope of application in terms of subject matter and scope of application and concern only selected areas, not even the IoMT itself, but also the IoT more broadly. Thus, regulations shaping IoMT user security may be classified into separate categories – as shown below:

- (1) Strictly “consumer” regulations: Directive 2011/83/EU.<sup>13</sup>
- (2) Safety regulations: General Product Safety Regulation;<sup>14</sup> Medical Device Regulation (MDR).<sup>15</sup>
- (3) Cybersecurity regulation: NIS Directive,<sup>16</sup> Cybersecurity Act.<sup>17</sup>
- (4) Provisions on the protection of personal data: General Data Protection Regulation.<sup>18</sup>

Although a fuller depiction of the EU’s model for regulating the cybersecurity of IoMT devices should be complemented by sectoral regulations, in my analysis, I will mainly focus on those acts that relate directly to the cyber and physical security of IoMT devices and that have a real impact on standard-setting for the connected products market.

#### 1. IoMT as a medical device under European Union law

IoMT is a broad category of devices of a strictly consumer nature (such as the extremely popular smartwatches), as well as those used in the clinical process. From a legal point of view, this distinction is of considerable importance, as the legislation in force in the European Union clearly distinguishes between devices that are medical devices and those that, despite their function, do not have such status,<sup>19</sup> which directly translates into the scope of obligations of manufacturers and their distributors, and thus also the level of protection of their users.

For those IoMT devices that are medical devices, the provisions of MDR on medical devices apply. The question then becomes which IoMT devices will correspond to the concept of medical devices?

According to the definition proposed by the EU legislator in Article 2 MDR, “medical device” means any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:

- (1) diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,
- (2) diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,

<sup>13</sup> Directive 2011/83/EU of the European Parliament and of the Council on consumer rights (2011) OJ L304/64.

<sup>14</sup> General Product Safety Regulation, Regulation (EC) No 765/2008, (2008) OJ L218/30.

<sup>15</sup> Regulation (EU) 2017/745 of the European Parliament and of the Council on medical devices, (2017) OJ L117/1.

<sup>16</sup> Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, (2016) OJ L194/1.

<sup>17</sup> 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, (2019) OJ L150/1.

<sup>18</sup> General Data Protection Regulation, Regulation (EU) 2016/679, (2016) OJ L119/1.

<sup>19</sup> Jarosław Greser, “Cyberbezpieczeństwo wyrobów medycznych w świetle rozporządzenia 2017/745” (2020) 2 Internetowy Kwartalnik Antymonopolowy i Regulacyjny 9, p 79.

- (3) investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,
- (4) providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations,
- (5) and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.

As Greser points out,<sup>20</sup> the concept of medical devices includes those IoMT devices that meet two types of premises together. The first premise is related to the form of impact on the patient, which includes tools, apparatus, devices, implants, reagents, materials or software. A medical device will not be a product that does not achieve its intended primary action through pharmacological, immunological, or metabolic means (in or on the human body), but whose action may be assisted by such means.

The second premise is related to the purpose of use of the device in question. Such a device must firstly be intended for human beings and secondly used for one of the purposes indicated in Article 2 MDR.<sup>21</sup>

In light of the above, there should be no doubt that wearable medical devices will not fall within the definition of medical devices referred to MDR, because they do not have the purposes indicated in the Regulation. Indeed, the data that the devices in question collect and then process are not subsequently used in the treatment process and are not assessed in terms of medical data. The assessment of whether an IoMT device is a medical device must therefore be made in each case by assessing whether the device serves a medical process.

In turn, those IoMT devices that fall into the MDR will have to guarantee the highest possible level of safety for patients, which the EU legislature intends to do by setting high quality and safety standards for medical devices and by laying down rules for the placing, making available on the market and putting into service in the Union.

The MDR defines a regulatory regime distinguishing four stages, each of which is of considerable importance for the overall safety of the user.

The first stage focuses on the placing of the device on the market and into use. Article 5 MDR provides that a device may only be placed on the market or put into service if, when duly supplied and properly installed, maintained and used in accordance with its intended purpose, it complies with this Regulation and must meet the general safety and performance requirements set out in Annex I relating thereto, taking account of the intended use of the device. Annex I specifies that the devices shall achieve the performance intended by their manufacturer and shall be designed and manufactured so as to be suitable for their intended use under normal conditions of use. The devices shall be safe and effective and shall not jeopardise the clinical condition or the safety of patients, the safety or health of users or, where appropriate, other persons, and any risks which may be associated with their use shall, when weighed against the benefits to the patient, represent an acceptable risk and shall be compatible with a high level of protection of health and safety, taking account of the generally acknowledged state of the art. In particular, it is a requirement to establish and maintain a risk management system, conduct clinical evaluation of the product, including post-market clinical follow-up, draw up and keep up to date the technical documentation, draw up the EU declaration of conformity and affix the CE conformity marking.<sup>22</sup> Manufacturers are therefore required to determine the intended use of the device, carry out clinical trials and performance

<sup>20</sup> Greser, (n 18), 82.

<sup>21</sup> Greser, (n 18), 82.

<sup>22</sup> Greser, (n 18), 85.

evaluation, establish a risk assessment and classify their medical devices according to a four-stage qualification system (ie Class I, IIa, IIb, III), where the higher the class the more stringent the product conformity assessment.

The second stage addresses the certification, review or marketing approval (marketing approval is required for devices classified as high or highest risk) which is based on the abovementioned information recorded in technical documents and submitted to the regulatory authority.<sup>23</sup>

Once a product has been placed on the market, the so-called third stage begins, namely the post-market surveillance: the manufacturer is obliged to ensure that the product remains safe and functions as intended, as specified in its original documentation.<sup>24</sup> Finally, manufacturers are also obliged to keep records and regularly report the results of post-market monitoring and surveillance to the regulator.

In the event that a device proves to be defective, or new risks to patient safety are detected or revealed, then the regulator is competent to withdraw the device from the market, which constitutes the fourth stage.<sup>25</sup>

The MDR also places certain categories of obligations on importers and distributors, not least in order to achieve greater compliance on the part of individual economic operators.

The previous short remarks seem to justify the thesis that the regulation introduces a set of mechanisms enhancing the safety of the medical devices themselves, including IoMT devices, and, by extension, of the persons using them. Of course, the scientific literature also draws attention to certain issues that may undermine the achievement of the objectives for which the regulation was adopted,<sup>26</sup> but, in principle, it must be assessed that the harmonised set of obligations for manufacturers provide grounds for affirming that, as Kosta Shatrov and Carl Rudolf Blankart rightly assessed, the MDR represents a pragmatic step in the right direction.

## 2. “Consumer” IoMT

For IoMT devices, which will not fall in the category of medical devices as defined by MDR, the regulatory environment addressing user safety includes several other pieces of legislation, including new pieces of legislation and legislative proposals that will directly relate to the Internet of Things, but also more specifically to those IoMT devices. Both legislation in force and proposed legislation will be considered in the remainder of this work, showing the conception of the EU legislator as to what the protection of users of IoMT devices should look like.

Directive 2001/95/EC on general product safety is the starting point. Article 1 clarifies that the directive aims to ensure the safety of all products placed on the market. Article 2 defines a product as any product – including in the case of a service – which is intended for consumers or likely, under reasonably foreseeable conditions, to be used by consumers even if not intended for them, and is supplied or made available, whether for consideration or not, in the course of a commercial activity, and whether new, used or reconditioned. This definition clearly applies to IoMT devices. By contrast, a “safe product” is considered to be any product which, under normal or reasonably foreseeable conditions of use including duration and, where applicable, putting into service, installation and

<sup>23</sup> Irina Brass, Andrew Mkwashi, “Risk Assessment and Classification of Medical Device Software for the Internet of Medical Things: Challenges arising from connected, intelligent medical devices” (2022) Proceedings of the 12th International Conference on the Internet of Things IoT ‘22). <https://doi.org/10.1145/3567445.3571104>

<sup>24</sup> Brass, Mkwashi, (n 23).

<sup>25</sup> *Ibid.*

<sup>26</sup> See the analysis conducted by Kosta Shatrov, Carl Rudolf Blankar, “After the four-year transition period: is the European Union’s Medical Device Regulation of 2017 likely to achieve its main goals?” (2022) 126 Health Policy 12, pp 1233–40.



maintenance requirements, does not present any risk or only the minimum risks compatible with the product's use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons. The following points should be considered:

- (1) the characteristics of the product, including its composition, packaging, instructions for assembly and, where applicable, for installation and maintenance;
- (2) the effect on other products, where it is reasonably foreseeable that it will be used with other products;
- (3) the presentation of the product, the labelling, any warnings and instructions for its use and disposal and any other indication or information regarding the product;
- (4) the categories of consumers at risk when using the product, in particular children and the elderly.

Under the Directive, producers are obliged to fulfill one general obligation to place only safe products on the market, as well as several other specific obligations, such as providing consumers with adequate information to enable them to assess the risks posed by the product during normal or foreseeable use, in the absence of adequate warnings of such risks, and to take appropriate precautions.

Furthermore, distributors are obliged to act with due care to ensure compliance with the applicable safety requirements. Furthermore, distributors, within the limits of their respective activities, should participate in monitoring the safety of products placed on the market, in particular by passing on information on the risks that products present, keeping and providing the documentation necessary for tracing the origin of products and cooperating with producers and the competent authorities on risk-avoidance measures taken. Within their field of activity, distributors should take measures to cooperate effectively.

Academic literature has observed that, although Directive 2001/95 applies to those products used by consumers that do not meet the requirement of health and safety protection, it does not define the very concept of safety – which further necessitated specific legislative steps in the individual Member States.<sup>27</sup> For this reason, among others, a new legislative proposal has been presented introducing clear and detailed provisions, leaving no room for differing transposition by Member States. Regulation (EU) 2023/988 on general product safety<sup>28</sup> has recently been adopted. This Regulation – as mentioned in Article 1(2) – lays down essential rules on the safety of consumer products placed or made available on the market. Significantly, the regulation defines product as any item, whether or not it is interconnected to other items, supplied or made available, whether for consideration or not, including in the context of providing a service, which is intended for consumers or is likely, under reasonably foreseeable conditions, to be used by consumers even if not intended for them. Again, this leaves no illusion that IoMT devices will fall within this definition. It should be noted that the EU legislator decided to define a dangerous product as any product which is not a “safe product” (Article 3(3)), and as a safe product any product which, under normal or reasonably foreseeable conditions of use, including the actual duration of use, does not present any risk or only the minimum risks compatible with the product's use, considered acceptable and consistent with a high level of protection of the health and safety of consumers (Article 3(2)).

<sup>27</sup> Cezary Banasiński, Marcin Rojszczak, “Cybersecurity of consumer products against the background of the EU model of cyberspace Protection” (2021) 7 *Journal of Cybersecurity* 1, pp 5–6.

<sup>28</sup> Regulation (EU) 2023/988 on general product safety (2023) OJ L 135/1.

Looking at the Regulation in the context of the IoMT, it is certainly noteworthy that the EU legislator has considered the case of Internet of Things and the risks arising from their use by explicitly pointing out that objects that connect with other objects, or non-integrated objects that affect the way another object works, may pose a risk to product safety. This aspect should be adequately addressed as a potential risk. The connections and interdependencies that an object may have with external objects should not compromise its safety.<sup>29</sup> The protection of the consumer using IoMT devices is also supported by the fact that the EU legislator has chosen to oblige all actors involved in the supply and distribution chain to take appropriate measures to ensure that they make available on the market only products that are safe and comply with this Regulation.

The adequacy of the IoMT user protection may be assessed by reference to the so-called “milestones” setting the standard of consumer protection, ie in particular provisions concerning the implementation of the information obligation, issues related to the assurance of fair contractual terms and conditions or consumer protection against unfair commercial practices.

With regard to issues concerning the implementation of the information obligation towards the consumer, the provisions of Directive 2011/83/EU are relevant in this regard. There is no doubt that an IoMT user who purchases a wearable medical device will fall within the definition of a consumer proposed in the directive. Undoubtedly, it can also be assumed that IoMT devices can be qualified as goods according to Directive 2011/83/EU, ie as any tangible movable item, with the exception of items sold by way of execution or otherwise by operation of law. At the same time, since there are no grounds to consider that the provisions of Directive 2011/83/EU will be excluded due to any of the circumstances indicated in Article 3 of the Directive, its provisions will therefore apply and shape the legal position of the IoMT user.

According to Articles 5 and 6 of the Directive, the assessment of the adequacy of the provisions shaping the duty of information in relation to IoMT devices is not clear-cut. While in the case of a purchase of an IoMT device, such as a smartwatch, many times, the consumer has an adequate level of protection, regardless of whether the contract is concluded at a distance or not, as regards such information as, for example, the identity of the trader, the conditions of payment, delivery, performance, the time limit within which the trader undertakes to deliver the goods or to provide the service, and the trader’s complaint handling procedure, in relation to the duty to provide information on the main characteristics of the product or the functionality of the digital content, this assessment may become significantly more complicated. This is due to an intrinsic feature of any IoT device, including IoMT devices, namely its functionality, which is the result of a complex network of interconnected applications and services and, ultimately, the input of the consumer himself.<sup>30</sup> This, in turn, makes it more difficult for the manufacturer to comply with its duty to provide information in such a way that the consumer can be deemed to have actually been informed of, for example, the functionality of digital content, etc.

The fairness of contractual terms are regulated by the Directive on unfair terms in consumer contracts, also in case of IoMT. The Directive addresses the non-binding nature of unfair contract terms and therefore aims to address the problem of “significant imbalance in the rights and obligations of the parties under the contract.” However, the specific nature of the IoMT, through the collection and processing of vast amounts of data about users and the associated detailed knowledge of consumers’ vulnerabilities, behaviours and biases, has the effect of significantly aggravating the imbalance of power

<sup>29</sup> Recital 24 General Product Safety Regulation.

<sup>30</sup> Natali Helberger, “Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law”, (2016) <<https://ssrn.com/abstract=2728717>> (last accessed 03 September 2023).



between users and producers of these devices.<sup>31</sup> In this context, it also seems relevant to address the question of the extent to which IoMT users will be able to safeguard their interests and negotiate fair terms, in order to ensure transparency, considering this widespread imbalance of power?<sup>32</sup> These contracts are, after all, mostly adhesion contracts, and the user may not even be interested in negotiating their terms and conditions if he is not aware of what market practices he is being subjected to.

The traditional consumer regime that goes beyond the contract and, as a principle, can be more helpful is the Unfair Commercial Practices Directive. Central to the directive is the autonomy of the consumers' decision-making process, providing protection against deception and unfair restrictions on consumer choices.<sup>33</sup> According to recital 18, the yardstick for unfairness is an average consumer who is sufficiently well-informed and reasonably attentive and cautious, taking into account social, cultural, and linguistic factors, in line with the interpretation of the Court of Justice. The directive also acknowledges that commercial practices may target vulnerable consumers, ie those ones particularly susceptible to such practices or the product in question, due to physical or mental disabilities, age, or gullibility. Determining the characteristics of an average consumer or an average representative of a specific group of consumers falls within the competence of national courts and can be challenging in practice, especially considering the specificity of IoMT. Following the insightful example given by Natali Helberger, where a purchaser of a smartwatch will need a different level of media usage skills, technical understanding, and awareness of basic legal implications than a purchaser of an "ordinary" analog watch,<sup>34</sup> in case of consumer IoMT devices, for consumers using contact lenses to measure blood glucose levels, the informational obligation should be fulfilled differently than for consumers using regular contact lenses.

As a result of the previous analysis, pre-contractual, contractual, and non-contractual protection for IoMT users are not without imperfections and certain legislative shortcomings. The following step is then evaluating to what is the extent consumers are protected when the IoMT device proves to be defective. This issue is addressed by the Directive 85/374 concerning liability for defective products. Nevertheless, the applicability of the provisions of this act to IoMT devices may be debatable for the following reasons.

Firstly, in the context of IoT, the definition of the product itself seems problematic: Article 2 states that a product means "any movable item, excluding agricultural raw materials and hunting and fishing products, even if it forms part of another movable or immovable item." "Product" also includes electricity. This definition was perceived as problematic when attempting to classify IoT devices as products under this directive until the European Commission provided for clarifications. The Commission stated that IoT devices and any other objects containing intangible elements or possessing communication features, provided they qualify as "movable items," are considered "products," and defects in these products are covered by the directive.<sup>35</sup> Thus, IoMT devices, which have the nature of movable items, will also be covered by this directive.

However, the functionality of intangible elements (software, etc.) is typically crucial in an IoT device. Such information transfer may be considered as a "service." According to the European Commission, such a service will not be subject to EU product liability and safety regimes.<sup>36</sup> Therefore, "in cases where damage is caused by the provision of incorrect

<sup>31</sup> Helberger, (n 31).

<sup>32</sup> *Ibid.*

<sup>33</sup> *Ibid.*

<sup>34</sup> *Ibid.*

<sup>35</sup> "Commission Staff Working Document, Liability for emerging digital technologies (2018) SWD 137 final."

<sup>36</sup> "What are the key legal considerations? Part of our Internet of Things briefing" (2019) <<https://www.insidetechnology.com/internet-of-things/what-are-the-key-legal-considerations#27>> (last accessed 12 November 2023).

data or the failure to provide data, assigning responsibility may become unclear, and claims potentially difficult to enforce. This means that sellers may consider placing key safety functions in the cloud to try to avoid product liability.<sup>37</sup>

Moreover, the definition of defective product is also considered problematic. According to Article 6, a product is defective if it does not provide the safety that a person is entitled to expect, taking into account all circumstances, in particular: the appearance of the product; the way in which the product is intended to be used, which can be reasonably expected; the time when the product was put into circulation. It is also stated that a product will not be considered defective solely because a better product was later introduced into the market. However, for the manufacturer to be legally liable, there must be a causal link between the product's defect and the resulting damage. Such an understanding of manufacturer liability does not fully align with the issue of security discussed here. For such an assessment, the provision of user instructions/warnings will be crucial. As IoT devices become increasingly sophisticated and technology advances, it will become more challenging to make the information provided on products sufficiently clear to enable consumers to assess the security of highly technically advanced products and understand the processes that enable their operation. When considering the choice of products to purchase, consumers are not always able to assess which one is truly safe.<sup>38</sup>

Regarding the issue of liability for defective products, the EU legislator has announced certain legislative changes that cannot be overlooked. On 28 September 2022, the Proposal for a Directive on liability for defective products<sup>39</sup> was published, aiming to establish a compensation system at the EU level for individuals who have suffered harm to health or property caused by defective products.

From the perspective of users, it is noteworthy, first and foremost, that consumer IoMT devices will fall within the concept of a product. According to the proposal, the concept of a product includes all movables, even if integrated into another movable or into an immovable. "Product" includes electricity, digital manufacturing files, and software. The proposal also adopts the principle that strict liability for defective products should apply to all movable items, including those integrated into other movable items or installed on them.<sup>40</sup> Additionally, in order to reduce the burden of proof for the plaintiff, the proposal obliges manufacturers to disclose evidence, aiming to ease the burden of proof on consumers in complex cases.

The proposed Directive, however, is not without shortcomings in the context of IoMT, as rightfully pointed out by Greser, who states that, "the proposal introduces a presumption of product defectiveness in certain situations. One of these is a claimant's establishment that a product fails to comply with mandatory safety requirements under EU or national laws that are designed to protect against the risk of damage. In such cases, it will not be possible to refer to noncompliance with nonlegal standards as a source of damage. This seems to be the wrong approach, considering the dynamics of changes in cybersecurity threats and, generally speaking, the more rapid adaptation of nonlegal standards to them."<sup>41</sup>

Summarising the above considerations regarding the level of protection for consumer IoMT users in light of EU legislation, a first consideration is the multitude of regulations shaping these issues. While this diversity of regulations *per se* is not necessarily negative,

<sup>37</sup> *Ibid.*

<sup>38</sup> *Ibid.*

<sup>39</sup> "Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM(2022) 495 final, 2022/0302(COD).

<sup>40</sup> Recital 6 of the preamble of the draft.

<sup>41</sup> Jaroslaw Greser, "A Step Forward in Health-related IoT Cybersecurity: Remarks on the Proposal for a Liability for Defective Products Directive" (2023) 5 *Front. Digit. Health* 1193255.

it brings about significant consequences. Such legislative “fragmentation” may pose problems for individual consumers in understanding their rights. For the average consumer, the proper interpretation of the relationship between various legal acts can also be challenging. At the same time, manufacturers and other entities offering such products must be vigilant regarding the existence of regulations about them across various legal acts.

The rapid technological transformation, including in the IoMT sector, requires constant monitoring of user protection levels in various fields. Any legislative changes often need to be coordinated at multiple levels and about multiple texts simultaneously. To address these concerns, especially in the cybersecurity domain, one of the recent initiatives undertaken by the European legislator appears to be the Cyber Resilience Act proposal.<sup>42</sup> This initiative currently addresses the unregulated cybersecurity market of IoT. Its goal is to establish basic security requirements for digital products and related services available in the EU.

The Cyber Resilience Act aims to contribute to ensuring that manufacturers enhance the security of products with digital elements. It seeks to establish cohesive cybersecurity frameworks, facilitating compliance for hardware and software manufacturers, while enhancing transparency regarding security features. Finally, it aims to protect businesses and consumers, enabling them to use these products safely.<sup>43</sup>

Under the proposed regulation, manufacturers will be obligated to conduct an assessment of the compliance of products with digital elements and procedures established by the manufacturer to determine whether the fundamental requirements specified in Annex I, which requires delivery “without any known exploitable vulnerabilities,” have been met. The proposed regulation will not apply to products with digital elements covered by the MDR.

It is positive to recognise the ever-increasing awareness on the part of the EU legislator regarding the changing context and conditions in which IoMT device users are expected to operate. This is particularly accentuated in recent years, especially with the dynamic technological advancements and the widespread adoption of such products on a mass scale. The hallmark of responsible legislative actions is a consistent and systematic orientation towards the needs of individuals, while simultaneously ensuring market balance.

Of course, examples of certain legislative shortcomings could be multiplied across various fields. However, the mere recognition of the necessity to revise many legal acts to enhance the security level for IoMT users creates a kind of “light at the end of the tunnel.” It is crucial to emphasise that this should be accompanied by an appropriate pace of legislative work.

#### **IV. The regulatory environment in the United States**

Transitioning to an analysis of the regulatory environment for consumer safety in IoMT in the United States, it is crucial to first note the similarities with the previously discussed legislation in the European Union.

Similar to the EU, the United States lacks a single legal act that comprehensively shapes IoMT regulations at the federal level. Additionally, akin to the European Union, certain categories of regulations can be distinguished in the US, covering product safety (including product liability regulations), strictly “consumer” regulations, as well as those pertaining to data protection and privacy. Of particular importance for the current analysis, the United States also has legal regulations concerning medical devices. This necessitates an

<sup>42</sup> Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

<sup>43</sup> Carsten Rhod Gregersen, “EU Cyber Resilience Act: the GDPR for IoT” (2023) <<https://www.embedded.com/eu-cyber-resilience-act-the-gdpr-for-iot/>> (last accessed 15 October 2023).

analysis and an attempt to answer the question of whether, and if so, to what extent these regulations will impact the protection of IoMT device users.

### ***1. Medical device as a category of IoMT in US law***

The primary source of legal regulations concerning medical devices in the United States is the Medical Device Amendments of 1976 to the Federal Food, Drug, and Cosmetic Act.<sup>44</sup> These regulations cover various aspects, including pre-market review, approval of medical devices, a risk-based classification system, requirements for good manufacturing practices, reporting adverse events, and requirements for medical device studies.<sup>45</sup> Over the years, this law has undergone multiple amendments through acts such as the Safe Medical Devices Act of 1990 (the 1990 Act), the Medical Device Amendments of 1992 (the 1992 Amendments), the Food and Drug Administration Modernization Act of 1997 (FDAMA), the Medical Device User Fee and Modernization Act of 2002 (MDUFMA), the Food and Drug Administration Amendments Act of 2007 (FDAAA), and the Food and Drug Administration Safety and Innovation Act (FDASIA) enacted in July 2012.<sup>46</sup>

The concept of medical devices is defined in Section 201(h) of the Food, Drug, and Cosmetic Act. The term “device” refers to an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article. This includes any component, part, or accessory that meets the following criteria:

- (1) Recognised in the official National Formulary or the United States Pharmacopeia, or any supplement to them.
- (2) Intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in humans or other animals.
- (3) Intended to affect the structure or any function of the body of humans or other animals.

Importantly, a medical device does not achieve its primary intended purposes through chemical action within or on the body of humans or other animals and is not dependent upon being metabolised for the achievement of its primary intended purposes.

The proposed definition of medical devices in US law undoubtedly encompasses a significant portion of IoMT devices, which, according to the earlier qualification presented, fall into the category of devices with a strictly clinical purpose. Firstly, the US legislator, by formulating “or other similar or related article,” used an open catalogue, which practically eliminates the need to determine whether IoMT devices will be considered a machine, contrivance, or another article. Secondly, it seems indisputable that at the current stage of IoMT device development, they do not utilise any chemical actions in the body or on the body, and the achievement of their intended purpose is not dependent on metabolism. Finally, they are used for diagnosing disorders or other medical conditions, as well as in the treatment or prevention of diseases. In a situation where an IoMT device meets these criteria, it should be classified as a medical device under the FDCA. An important variable in this regard is that the manufacturer’s intention is the key factor determining the status of the “product.” Manufacturer declarations regarding the product define the “intended use,” and the same product may be a device or not, depending on the manufacturer’s

<sup>44</sup> Medical Device Amendments of 1976 to the Federal Food, Drug, and Cosmetic Act, Pub. L. No. 94-295, 90 Stat. 539 (1976).

<sup>45</sup> Ellen J. Flannery, “Overview of the Legal Framework for Medical Device Regulation in the United States,” *Medical Devices Law & Regulation* (2017), p. Q 1.2, <[https://legacy.pli.edu/product\\_files/Titles/4661/%23172971\\_Medical%20Devices%20Law%20AB%202017\\_20161028150449.pdf](https://legacy.pli.edu/product_files/Titles/4661/%23172971_Medical%20Devices%20Law%20AB%202017_20161028150449.pdf)> (last accessed 21 September 2023).

<sup>46</sup> Flannery, (n 46).

declaration. As an example, following Ellen J. Flannery, one can point to a situation where exercise equipment used for maintaining good health may not be considered a device, while the same equipment designed for the cardiac rehabilitation of patients after heart surgery will be considered a device under the FDCA.<sup>47</sup>

If an IoMT device is considered to meet the criteria for a medical device, the FDCA establishes regulatory frameworks for these products based on risk analysis. According to Section 513 of the FDCA, products are classified according to the level of risk. Similar to the EU approach, US legislation distinguishes three risk classes. In practice, as indicated by statistical data, more devices in the EU fall into risk class I (40% versus 35%) and risk class III (16% versus 9%) compared to the US. The US has more devices in risk class II, accounting for 53% compared to 44% (combining Class IIa and IIb) in the EU.<sup>48</sup>

In the United States, like in the European Union, Class I applies to medical devices posing the least risk and subject to general controls specified by law. Class II devices are subject to both general and special controls. Consequently, nearly all Class I devices and some Class II devices are exempt from premarket review. However, most Class II devices (and some Class I devices) can enter the market only after FDA approval through a premarket notification, pursuant to Section 510(k) of the law. This pathway requires the device to be “substantially equivalent” to a “predicate device.” A predicate device is a similar product introduced to the market before 28 May 1976 (the enactment date of the amendments) or introduced after that date and deemed by the FDA to be substantially equivalent to a legally marketed device previously cleared through a 510(k) submission. Most devices are marketed through this pathway and the premarket notification is referred to as a “510(k) submission.”<sup>49</sup> Comparing this procedure with the provisions of Regulation 2017/745, it can be assessed that the criteria for demonstrating equivalence are less stringent.<sup>50</sup>

On the other hand, Class III devices, such as implants and life-supporting devices, are subject to the most rigorous controls, including approval before market entry by the Food and Drug Administration (FDA).<sup>51</sup> Class III devices, including those that are not substantially equivalent to a predicate device, cannot be marketed until: (1) the device has been tested for safety and effectiveness; (2) a premarket approval (PMA) application has been submitted to the FDA; and (3) the FDA has approved the PMA as demonstrating sufficient assurance that the device is safe and effective for its intended use. The FDA may impose conditions on the approval of the PMA, including post-approval study requirements and restrictions on sale, distribution, or use.<sup>52</sup>

Indeed, the FDA’s responsibility regarding the clearance of medical devices before their introduction to the market is to assess their safety, effectiveness, and quality (in accordance with good manufacturing practices).<sup>53</sup>

For all users of IoMT devices, the inclusion of these devices in a classification system, taking into account the level of risk associated with their use, seems to be a favourable circumstance on the path to ensuring an adequate level of protection. However, it should be noted that due to various factors such as uncertainty, delays, and the costs associated with FDA actions before introducing a product to the market, the risk of either complete discouragement of innovation or slowing it down increases. This could result in potential benefits emerging with delay or in other countries.

<sup>47</sup> Flannery, (n 46).

<sup>48</sup> Matthias Fink, Bassil Akra, “Comparison of the international regulations for medical devices—USA versus Europe,” *Injury* 54 (2023), 2.

<sup>49</sup> Flannery, (n 46).

<sup>50</sup> Fink, Akra, (n 49) 3.

<sup>51</sup> Flannery, (n 46).

<sup>52</sup> *Ibid.*

<sup>53</sup> Richard Williams, Robert Graboyes, and Adam Thierer, “US Medical Devices: Choices and Consequences,” (2015), 44 <<https://www.mercatus.org/system/files/Williams-Medical-Devices.pdf>>, (last accessed 21 September 2023).



In reality, the FDA is unable to keep up with the rapid technological development, as Larry Downes pointed out, stating that “technology changes exponentially, but social, economic, and legal systems change gradually.” The FDA verification process is almost twice as long as that of its European counterpart (the European Medicines Agency) for devices that do not require clinical data and almost three times longer for devices requiring clinical data.

When CEOs of medical device manufacturing companies were asked about their biggest challenge in 2014 (in the United States), over 43% responded that it was the “changing regulatory environment.” In fact, the United States was the second most challenging market for introducing new medical devices, second only to China.<sup>54</sup>

In the USA, unlike in the EU, as discussed earlier, for most devices, the FDA requires only general post-market actions, such as gathering opinions from physicians or accessing the MAUDE database. In March 2023, 21 ongoing studies post-market introduction were listed in the database.<sup>55</sup>

Referring to IoMT medical devices, it is noteworthy that in 2023, the US legislature took significant steps to enhance their cybersecurity. The observation of a reality where open-source software became a significant part of many medical devices prompted legislative action. As a result, in December 2022, the FDA signed the Consolidated Appropriations Act 2023,<sup>56</sup> also known as the “Omnibus.” Section 3305 of the Omnibus, titled “Ensuring Cybersecurity of Medical Devices,” amended the Federal Food, Drug, and Cosmetic Act [FD&C Act] by adding section 524B: “Ensuring Cybersecurity of Devices.” This amendment became effective in March 2023 and requires the sponsor of a premarket submission for a cyber device to submit a plan for monitoring, identifying, and addressing any post-market cybersecurity vulnerabilities and exploits. Devices that do not meet the specified legal requirements will be deemed inadmissible and will not enter the market.<sup>57</sup> The Government Accountability Office will be tasked with collecting and reporting challenges related to the adoption and implementation of regulatory requirements.

In the United States, the aforementioned legislative action took place at a time when the European Union was in the process of developing the Cyber Resilience Act. It appears that its provisions may be more stringent. The reason for this is because it would subject manufacturers introducing devices in the EU to a new set of criteria aimed at ensuring safer hardware and software. This includes establishing processes and actions to prioritise safety at every stage of the product life cycle.<sup>58</sup>

## 2. IoMT and product liability regulations

Apart from the previously mentioned acts that regulate medical devices and IoMT in state law, the regulatory landscape for the safety of IoMT users will also be shaped by product liability laws.

As Amodio points out,<sup>59</sup> there is no federal law on product liability, various states have enacted regulations in this regard, and these regulations vary depending on the state and product category. Referring to the definition in the Third Restatement of Torts, Amodio

<sup>54</sup> Williams, Graboyes and Thierer (n 55).

<sup>55</sup> Fink, Akra, (n 49) 4.

<sup>56</sup> Consolidated Appropriations Act, H. R. 2617, House of Representatives (2023).

<sup>57</sup> Trustonic, “Why the FDA’s Medical Cybersecurity Ruling is Good News for Device OEMs” (2023) <<https://www.trustonic.com/opinion/why-the-fdas-medical-cybersecurity-ruling-is-good-news-for-device-oems>> (last accessed 12 November 2023).

<sup>58</sup> Winston Leung, “New FDA Medical Device Cybersecurity Requirements and How to Simplify Compliance” (2023) <<https://blogs.blackberry.com/en/2023/06/new-fda-medical-device-cybersecurity-requirements>> (last accessed 12 November 2023).

<sup>59</sup> Lucas M. Amodio, “The Intersection Of Product Liability Law And The Internet Of Things” (2021) <<https://lira.bc.edu/work/ns/ec719455-082a-448b-bf19-b70eb31aa0de/reader/6945da64-72bc-4a49-9f27-7b1d6aa40bbf>>, 12.



identifies three categories of product liability: manufacturing defects, design defects, and inadequate instructions or warnings.

In general, three main theories of liability defined by common law include breach of warranty, negligence, and strict liability. Amodio suggests that product liability law could serve as a means to protect IoT consumers from physical damage caused by malicious hacking attacks. If a hacker successfully damages a user's IoT device, the user should be able to file a complaint against the manufacturer and the installer. If the security of the breached system does not meet the reasonable cybersecurity standard outlined by the FTC (Federal Trade Commission), the user should be able to plead negligence, arguing that the lack of or low security was a defect in the device and the "but for" cause of their injury. Amodio acknowledges that while no security setup can prevent all hacking attempts, manufacturers may use the FTC's reasonable cybersecurity standard as a guideline for securing the devices they manufacture. This standard of care would encourage manufacturers to take reasonable precautions and stay informed about the latest developments in security, ultimately protecting consumers in the long run. Additionally, making manufacturers entering the IoT space aware of the risks of liability would help ensure that the security of IoT products is taken seriously.<sup>60</sup>

In the context of IoMT devices, Bethany A. Corbin also expressed the belief that fitting traditional tort doctrine to the reality of IoMT is akin to fitting a square peg in a round hole.<sup>61</sup> One reason for such an assessment is the ambiguity regarding whether software is considered a product or a service. Products liability applies only to products, and in some U.S. states, software or code may be perceived as an intangible item. Due to the variability in products liability standards across the United States, there is a possibility that some jurisdictions may find strict products liability inapplicable to insecure code. Consequently, strict products liability may not offer a sufficient remedy for consumers despite the potential harm posed by insecure IoMT code.<sup>62</sup> Additionally, attention is drawn to the potential lack of clarity in assigning responsibility for the faulty operation of the device within the supply chain, as there is currently no clear delineation of responsibility in this chain. This issue is further compounded in the case of IoMT, which involves numerous manufacturers, developers, suppliers, programmers, and sellers.<sup>63</sup>

## V. Concluding remarks

In the year 2010, in one of the earliest legal scholarly works dedicated to the phenomenon of the Internet of Things, Rolf H. Weber and Romana Weber highlighted the necessity of creating legal frameworks for this, then still nascent, technology.<sup>64</sup> As correctly observed at that time, the establishment of an appropriate regulatory environment would ensure a sufficient level of security for the entire IoT structure, as well as the privacy of its users.<sup>65</sup> The above statement, of course, also applies to the IoMT.

The analysis conducted in this paper could be summarised with the truistic statement that the law lags behind technology. However, in the author's assessment, this would be too much of a simplification. There are indeed several solutions that should be evaluated positively, such as the existence of separate regulations for medical devices in both the European Union and the United States. These regulations impose higher obligations on the manufacturers of these devices and extend their scope to cover some IoMT devices.

<sup>60</sup> Amodio, (n 61) 24–25.

<sup>61</sup> Corbin, (n 7) 20.

<sup>62</sup> *Ibid.*, 22.

<sup>63</sup> Corbin, (n 7) 23.

<sup>64</sup> Rolf H. Weber and Romana Weber, "Internet of Things: Legal Perspectives" (2010), 3.

<sup>65</sup> *Ibid.*

Beneficial for IoMT users is also the situation where both EU and US legislation grant them mechanisms for protection and enforcement of their rights when they act as consumers in their relationships with manufacturers. This significantly limits the spaces within IoMT that may escape either EU or US legislation. On the other hand, this paper has highlighted certain deficiencies that should be addressed in the future, as they may adversely affect the level of protection for IoMT users. Although this analysis did not cover many other legally relevant acts in this area, it allows us to conclude, paraphrasing the words of R. and M. Weber, that IoMT is no longer an emerging technology today, and the law in this area seems to be maturing.

**Competing interests.** The author declares that there is no conflicts of interests.