European Journal of Risk Regulation (2024), **15**, 912–927
doi:10.1017/err.2024.68

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Mixed-Functions IoT devices: a Regulatory and Liability Requirements' Maze. A First Overview

Francesca Gennari

Sant'Anna School of Advanced Studies
Email: Francesca.Gennari@santannapisa.it

Abstract

This early-stage research article intends to explore the regulatory and liability requirements of a not yet fully developed subset of consumer Internet of Things (IoT) objects: the mixed-functions IoT devices. These objects could be wearables or not but could perform an e-health function, such as measuring your heartbeat, as well as consumer functions, such as displaying chat notifications. I argue that these mixed-functions devices will play an important role within smart homes as they will interact with new medical IoT devices to carry on rehabilitation and other medical functions at home. That is why it is important to start mapping down all the regulatory and liability requirements that might interest mixed-functions IoT device developers for them to understand which thread to follow in this regulatory and liability requirements maze.

Keywords: AI; IoT; liability; safety requirements

I. The rise of mixed-functions IoT objects: what they are and why they are relevant for the next generation of medical devices

This early-stage research article aims to explore the regulatory and liability requirements of a not yet fully developed subset of Internet of Things (IoT) objects: the mixed-functions IoT devices, which combine consumer and health related services. These products could be wearables or stationary devices, with incorporated software, but their essential feature is that they can perform an e-health function, such as measuring your heartbeat, as well as a consumer function, such as displaying chat notifications. Although the average user might consider mixed-functions IoT objects to be medical devices, regulators view them as consumer objects. This is not without consequences, as there are many differences in the substantive and procedural rules to market a product depending on whether it is a consumer object or a medical device. This article aims to deal with the ambiguity of what an e-health function is: *de facto* it could be one of the functions that are described as "medical" by Article 2 of the Medical Device Regulation (MDR)[1], such as diagnosis or vitals monitoring, but it is performed -even non-simultaneously- together with other ones (e.g.

[1] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017].

OJ L 117/1. The same Art 2 MDR not only describe medical functions, including diagnosis, monitoring and rehabilitation but also what can be defined as a medical device in very general terms. The same article recites that 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*

email notifications) that are typically consumer functions, such as calendar notifications. These e-health and consumer functions can coexist within a consumer object which is not a medical device because of two reasons. First, the MDR does not foresee the combination of different functions apart from the medical ones listed in Article 2 MDR. Second, it is up to the manufacturer to decide whether or not to market the device as a medical one. Ultimately, this last decision is part of the manufacturer's choices for which they need to be accountable and responsible.

The mixed-functions IoT objects such as smart watches or integrated voice assistants are at a crossroads between medical and consumer functions. Despite being consumer objects from a regulatory point of view, I argue that these mixed-functions devices will play an essential role within smart homes as they will be used by an increasingly older but digitally literate generation. These mixed-functions objects will enable people to carry on rehabilitation and other medical functions at home as they will get more and more interoperable with certified medical devices, included IoT ones. That is why it is important to start mapping down all the regulatory requirements and liability rules that might interest mixed-functions IoT device manufacturers. It will be important for them to understand how to navigate in this regulatory and liability requirements maze.

I will first explain more in detail what the mixed-functions IoT objects are, and describe the methodology employed (1.1); then I will highlight the social significance of this hybrid category if IoT objects (1.2) and then focus on the liability as the *fil rouge* of the article (1.3). The second section of the article focuses on the diversity and potentially high number of requirements that are – or soon will be – mandatory for mixed-functions IoT objects by analysing in particular the recently approved Artificial Intelligence Act and a group of product safety regulations (2.1 and 2.2). These two kinds of regulatory sources are essential to clarify the additional obligations that do not only pertain to compliance, but will also influence the application of liability rules. In the third section, I will delve into the analysis of the proposals concerning liability which might apply to both mixed-functions IoT devices and IoT as medical devices. These proposals are better known as the product liability directive update[2] (PLDU)(3.1) and the AI civil liability directive proposal[3] (AILDP) (3.2). Given that mixed-functions IoT are used more and more in combination or by being powered by AI systems, the interplay between these two proposals will affect the choices of IoT manufacturers. Although contractual liability issues are also relevant, this article will only focus on extra-contractual liability. Finally, section 4 will draw preliminary conclusions on the liability regime of mixed-functions IoT devices.

1.1. What are mixed-functions IoT objects? A methodological explanation

It is important to explain the meaning of the expression mixed-functions IoT objects. As a preliminary remark, the IoT technology is extremely adaptable as it consists of creating

purposes a series of objects that could be considered medical devices, including software". More on the division between medical and non-medical devices infra and at subsection 1.1.

[2] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products COM/2022/495 final. On 12 March 2024, the European Parliament agreed on a new text but it is still not approved by the Council to this day. This is why the reference for this text will be the official proposal. Martina Vass, Yasmina Yakimova, "Defective products: revamped rules to better protect consumers from damages" (European Parliament official website, 12 March 2024) < https://www.europarl.europa.eu/news/en/press-room/20240308IPR18990/defective-products-revamped-rules-to-better-protect-consumers-from-damages> accessed 21 May 2024.

[3] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) COM/2022/496 final.

objects connected with sensors to a cloud system where a reply is elaborated in response to an input received from the sensors.[4] Let us start with some examples of IoT as medical devices and then some examples of mixed-functions IoT devices to better clarify what legal regime is applicable to each of the abovementioned groups. IoT objects can be medical devices such as real-time monitoring vests. In this case, an IoT is considered from a regulatory point of view as a medical device because its functions fall within the ones described by Article 2 MDR and because the IoT manufacturer decides to follow the MDR rules concerning the safety certification of medical devices to market it into the EU. The MDR is a special safety regime compared to the general objects' safety rules applicable in the EU (infra 2.2). Instead, the general objects safety rules apply to consumer objects. It goes almost without saying that IoT devices can also be marketed as consumer objects. Think about a home cleaning robot as an example of a consumer IoT application. The objective of the application of consumer safety rules is to obtain an EU conformity certification (CE) as well as in the case of medical devices. Nevertheless, the rules to follow in this last case are less streamlined and strict than in the case of medical devices. This article wants to investigate the private law liability issues concerning an emerging third category of IoT objects which formally are consumer ones, hence they follow the so-called, consumer law *acquis* (including the general safety regulations), but they do have a non-certified/certifiable medical function which in this article will be called e-health function.

Let me make an example to make things clearer. A smartwatch can be defined as an Internet of Things (IoT)-powered object. Usually, devices like smart-watches are called "wearables," which are "*miniaturised electronic devices that can be easily donned on and off the body or incorporated into clothing or other body-worn accessories*"[5] but this does not mean that all IoT objects are wearables. Following with the same example, a smartwatch not only tells you the time, but also becomes part of your daily routine. Some models can track down your vitals (e.g. your heart rate or the steps you take daily through the help of sophisticated sensors) and provide services such as displaying push-up notifications for emails received and calendar appointments. Sometimes, they can inform you of an altered and potentially dangerous health risk or call the emergency number on your behalf.[6]

The difference between two objects such as the smartwatch and a monitoring IoT vest might be non-existent for an average consumer/patient, but it is an important one in terms of certifications and regulatory frameworks. In the first case, the object is considered a consumer object despite its e-health function. This category of devices is subject to CE certification, which can be obtained by complying with the rules on the safety of products. Tracking down your vitals and signalling a potential health risk is an e-health function because the object is marketed as a consumer object. I cannot say that those functions are medical ones as they are not performed by an object certified as a medical device. However, they might have *de facto* the same function. In the IoT vest case, the object is a proper medical device and follows different certification paths for its safety of use.

[4] Debasis Bandyopadhyay and Jaydip Sen, "Internet of Things: Applications and Challenges in Technology and Standardization" (2011) 58 Wireless Personal Communications 49.

[5] Matthew Smuck and others, "The Emerging Clinical Role of Wearables: Factors for Successful Implementation in Healthcare" (2021) 4 npj Digital Medicine 1.

[6] After the first commercialisation of watches such as Apple watches it was not unusual to witness articles describing how a smart-watch alarm was conducive to save a person's life or able to predict a Covid-19 infection. As an example see Megan Cerullo "Smartwatches can help detect COVID-19 days before symptoms appear," *CBS News* (15 January 2021)< https://www.cbsnews.com/news/covid-symptoms-smart-watch/> accessed 21 May 2024. Lately the views on the medical prowess of these devices have been more nuanced. See for instance *contra* Rabdi Hutter Epstein, "Can a smartwatch save your life?" *The New York Times* (New York 20 May 2021). <https://www.nytimes.com/2021/05/20/well/live/smartwatch-heart-rate-monitor.html> accessed 21 May 2024.

In this article, as a methodological choice, I will deal mainly with the EU policy proposals and legal acts concerning IoT objects with both e-health and consumer functions. The smartwatch case, to be clearer.

Investigating the regulatory and liability schemes of this emerging kind of connected objects is important because two relevant and consequent issues could be developing soon. The first one is the creation of a regulatory gap: if mixed-functions IoTs are treated as simple consumer objects even when they do have an e-health or *lato sensu* medical function (such as vitals monitoring) the risk is that the application of EU consumer and general safety rules will create a lower standard of protection for life and health than the one that is provided by the MDR. The second issue is a consequence of the previously cited regulatory gap: if mixed-functions IoTs cause damage to consumers, then the application of product liability or AI liability rules (applicable or soon to be applied) must at least be easier for consumers (see infra 3.2 and 3.3).

1.2. The importance of mixed-function IoT devices: a multi-layered explanation

It is important to focus on this new branch of IoT devices because both the regulatory and liability issues mentioned before are caused by the interconnection of several factors. The first factor concerns the ties between regulation and interoperability which might give rise to incentives to design IoT objects that are the most interoperable possible, regardless of their functions. Scholars have already spotted a pattern in the EU digital policy where interoperability seems to be one of the most sought-after results by mentioning and requiring harmonized standards, common specifications, and self-certification schemes.[7] Soon, the substantial common core of these definitions could play a role in eroding the distinction between consumer IoT and medical devices as the ways of functioning and operating between the two might become *de facto* the same. As a secondary effect, it could also play a role in making the distinction between "traditional/ex-post" liability and "ex-ante" risk management and compliance more nuanced (see infra in 1.3).

The second factor to keep in mind while explaining the future rise of mixed-functions IoT objects concerns technology development boosted by the pandemic. As an example of this, let us think about how the most acute phase of the COVID-19 pandemic accelerated innovation and technologies that had already been present for years[8]: telemedicine and health monitoring became more widespread in just some months' time.[9] Also, there was an increase in making homes smarter, by relying on integrated voice assistants which could be the interface with the security of the home (e.g. smart cameras and alarms) but also energy (e.g. thermostats, shutters, and fridge controls).[10] These first two markets are both booming[11] and there might be a space for a new market which connects them.

[7] Hans Micklitz, "The Role of Standards in Future EU Digital Policy Legislation: A Consumer Perspective" <https://www.beuc.eu/reports/role-standards-future-eu-digital-policy-legislation-consumer-perspective> accessed 21 May 2024.

[8] Nada Y Philip and others, "Internet of Things for In-Home Health Monitoring Systems: Current Advances, Challenges and Future Directions" (2021) 39 IEEE Journal on Selected Areas in Communications 300–2.

[9] Steve Rogerson, "Digital health investments surge 79 per cent" imc, IoT M2m council (25 April 2022) <https://www.iotm2mcouncil.org/iot-library/news/connected-health-news/digital-health-investments-surge-79-per-cent/> accessed 21 May 2024.

[10] The prominent role of voice assistants was proved already by the report by the European Commission report on the sector inquiry on consumer internet of things COMMISSION STAFF WORKING DOCUMENT Accompanying the document REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Final report - Sector inquiry into consumer Internet of Things SWD/2022/10 final (127).

[11] As far as the home IoT objects see Osservatorio Internet of Things, L'Internet of Things alla prova dei fatti: il valore c'è e si vede! (Milano: Politecnico di Milano 1863 School of Management and osservatori.net digital innovation, 2021),12–13. On the one hand, there are new projects funded across Europe such as the NRRP-funded projects BRIEF and Fit4MedRob in Italy whose purpose is to create a new generation of therapeutic and medical

In fact, this new generation of medical devices and the smart-home IoTs often need a link (another IoT device most of the time) to work together. The solution is building mixed-functions IoT objects which could play mostly an intermediary role between smart home appliances (e.g. voice assistants for the home) and the new generation of medical devices (e.g. medical IoT such as monitoring vests). However, there could also exist mixed-functions IoTs which could be an interface with a doctor or a medical structure, such as the case of the smartwatch I mentioned before. This technological evolution is consistent with Mark Weiser's idea of "Ubiquitous Computing," which is a state in which computing power and applications are so close to us that are almost invisible.[12] This idea was also applied to the home environment in the early 2000s.[13] The phenomenon of technological convergence, which means the combination of different technologies,[14] has been blurring the boundaries among the latest years' cutting-edge technologies: Artificial Intelligence (AI) systems work in the cloud to analyse and react to the inputs collected at a device level from an IoT object. An example is how we interact with an integrated voice assistant such as Google Home, Alexa or Bixbi: we give a voice command; the speaker (sensor level) collects personal data[15] and sends them to a proprietary cloud where complex algorithms translate the input and elaborate a reply.

The third factor to consider is partially a consequence of the previous two: allowing and incentivising interoperability between different IoT objects by regulation, increasing development of smart-home and smart-rehabilitation objects and programs, and, most importantly, increasing the importance of the interface part of mixed-functions IoT objects, will make the traditional distinction between medical and consumer IoT devices more and more unclear, if not useless. In a few years, medical device developers might be tempted to make their e-health solutions interoperable with the IoT objects for the home. Moreover, even creators of IoT applications for the home or mixed-functions IoT manufacturers might be inclined to embed more developed e-health set of functions in their connected objects, which could be used in conjunction with a proper and technologically advanced medical device. Theoretically, this is the European Health Data Space's (EHDS) field of application.[16] In this way, even the patient/consumer might be facilitated in making their home also an effective rehabilitation centre. This process might already be in its early days: in 2022, Amazon bought a chain of private medical clinics and it is also one of the most famous manufacturers of IoT products for the home.[17] It is realistic

devices to ensure that rehabilitation and other kinds of physical therapies can be carried out with consistency and efficiency outside the hospital, mostly at the patients' home through the means of medical IoT, exergames or augmented reality. See "NRRP, Sant'Anna School first for research infrastructure: over 24 million for BRIEF, the project that coordinates to enhance a network of research infrastructure in Biorobotics. More than 15 million invested in the Pisa and Pontedera facilities" (Sant'Anna School of Advanced Studies 18 July 2022) <https://www.santannapisa.it/en/node/131961> accessed 21 May 2024. 'Fit4MedRob: fit4Medical Robotics' (Fit4MedRob website) <https://www.fit4medrob.it/> accessed 21 May 2024.

[12] Mark Weiser, "The Computer for the 21st Century" (1999) 3 ACM SIGMOBILE Mobile Computing and Communications Review 3.

[13] W Keith Edwards and Rebecca E Grinter, "At Home with Ubiquitous Computing: Seven Challenges" in Gregory D Abowd, Barry Brumitt and Steven Shafer (eds), *Ubicomp 2001: Ubiquitous Computing* (Springer 2001).

[14] Gerry Kranz, "Technological Convergence," *Tech Target* <https://www.techtarget.com/searchdatacenter/definition/technological-convergence> accessed 21 May 2024.

[15] Our voice is personal data according to CNIL, the French data protection health authority. CNIL, *A votre écoute* (CNIL 2020) 5 <https://www.cnil.fr/fr/votre-ecoute-la-cnil-publie-son-livre-blanc-sur-les-assistants-vocaux≥ accessed 21 May 2024.

[16] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space COM/2022/197 final.

[17] Karen Weise 'Amazon to acquire One Medical clinics in latest push into health care' *The New York Times* (New York, 21 July 2022) <https://www.nytimes.com/2022/07/21/business/amazon-one-medical-deal.html> accessed 21 May 2024.

to expect that Amazon's Alexa might become interoperable with private telemedicine applications or IoT medical devices developed by or for the chain of medical clinics, thus making mixed-functions IoT devices more popular and more widespread. In the EU, the same thing might happen, but things might different because of the current strict division between medical devices and consumer objects rules.

1.3. Mixed-functions IoT and private law liability rules

In the previous subsections, it was clarified that mixed-functions IoT devices are always consumers' objects according to today's EU regulatory approach. Hence, in terms of EU tort liability, if manufacturers do not comply, the rules on strict liability (the product liability directive[18] and, prospectively, its update, the PLDU) and the future AI liability directive proposal (AILDP) will apply. It is still unclear whether these two regimes are fit for mixed-functions IoT and their fast-paced evolution (more infra in 3.1 and 3.2).

However, if we understand liability with a larger meaning to encompass accountability as well, it will be impossible not to mention, even briefly, the multi-layered structure of compliance duties which mixed-functions IoT manufacturers will need to face ex-ante and for which they will be held accountable and, eventually, liable in case of damages to consumers (infra 2).[19]

The ensuing structure of the article will start from the two main assumptions stated in this first section: if it is true that interoperability and technological convergence are making distinctions between IoT as medical devices and consumer objects less clear, then it might be useful to know what the main regulatory acts applicable *ex-ante* to mixed functions IoT objects are. I am convinced that only by mapping down the legislative acts that a manufacturer needs to be compliant with *ex-ante* (sect. 2), it will be possible to clarify what consequences there will be in terms of *ex-post* private liability rules (sect. 3). From the combination of these concise regulatory and legislative maps, I hope that the EU legislators might take notice of the gaps that will be likely to be apparent in the upcoming years and that will concern common-use objects with a hybrid nature (sect. 4).

2. The maze part I. The regulatory requirements of the mixed-functions IoT

This section concisely reports which regulatory legislative acts are going to impact the design and the concrete assembling of mixed-functions IoTs. There will be a focus only on the upcoming AI regulation (2.1), and on the so-called product safety laws, as they are sources of regulatory requirements that have more connections with the liability fil rouge that I will deal with in section 3.

2.1. AI regulation

On 13 March 2024, the EU institutions adopted an agreement concerning a horizontal and general regulation aiming at the different forms of AI that are being developed and the ones that have existed for quite some time. This proposal was known since the beginning

[18] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products [1985] OJ L 210/29.

[19] This article focus on mixed-functions IoT devices as consumers' objects, accordingly the analysis of the liability rules in the following sections will start from the premise of an existing contractual relationship between the consumer and the manufacturer. This, however, does not exclude the possibility for third parties injured by the defective product to pursue an action on the basis of the set of rules of the Product Liability Directive Update.

as the AI Act (AIA).[20] The main rationale underpinning this regulation is two-fold. On the one hand, there is a fundamental rights protection rationale from also the legitimate uses of AI systems.[21] On the other hand, as in the GDPR, the AI act follows a risk management rationale.[22] This means that the higher the risk for EU citizens is from the AI systems employment, the more the AI systems providers will need to comply with ex-ante duties such as the certification of high-risk AI systems with specialised audit and certification bodies, called Notified Bodies,[23] and the need to train data by respecting the transparency principle[24] or by ensuring a meaningful "human oversight."[25]

The AIA relevance for the IoT objects, including the mixed-IoT is apparent from the provision referring also to "*product manufacturers placing on the market or putting into service an AI system together with their product and under their own name or trademark.*"[26]

It is indeed relevant to mention the new categories of AI systems as some of mixed-functions IoTs might already use one or more kinds of AI systems. The new AIA regulates AI systems (primarily intended as software)[27] in three categories: prohibited AI systems,[28] high-risk AI systems,[29] and general-purpose AI (GPAIs).[30] There is also a not-explicitly mentioned fourth category which comprehends all the AI systems that do not fit in the previously mentioned category and that are considered low-risk (more *infra*). GPAIs is a category that refers to foundation models which are mainly known as the technology behind chatbots such as Chat-GPT or Gemini which was the core of the AI act negotiations from end of 2022 until the AIA approval. It is relevant to mixed-functions IoTs as many integrated voice assistants are now using foundation models to train and function. The AIA then further divides the GPAIs systemic risk and non-systemic risks GPAIs with different compliance burdens depending on the ability to generate a systemic risk.[31] It is not yet clear however how we can tell if a GPAI can cause a systemic risk given their "general" and "unfinished" core which makes them able through the training and scaling technique to adapt to different tasks[32]. This means that there is no reasonable way to exactly know in advance whether a GPAI can cause a widespread risk to fundamental rights. Both the reasonable foreseeability and the violation of fundamental rights are the two conditions requested by the "systemic risk"[33] definition.

[20] As to this date (22 March 2024), there is still not a Eurlex published AIA text and the initial 2021 proposal. That is why for the present analysis we will use the latest adopted text and not the April 2021 proposal. Specifically, the EU parliament adopted the final AIA text on 13 March 2024 and it just needs to be published on the official journal. As there is still not a EUR-Lex test, the Parliament text was used as it is the most recent one and can be found here <https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html> accessed 21 May 2024. After the final acceptance of this paper, in July 2024, the final AIA version was published in the EU and it is freely available on EUR-Lex Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) PE/24/2024/REV/1OJ L, 2024/1689, 12.7.2024.

[21] Recital 1 AIA and Art 1(1) AIA.

[22] Recital 1 AIA and Art 1(2) AIA.

[23] Arts 23- 39 AIA.

[24] Art 13 AIA.

[25] Art 14 AIA.

[26] Art 2(1)(e) AIA.

[27] The definition considers the OECD definition and can be found at Art 3(1) AIA.

[28] Art 5 AIA.

[29] Art 6 AIA + Annexes II and III.

[30] Art 3 (63) and (66) and Chapter Ve AIA.

[31] Chapter V AIA and Annexes XI- XIII.

[32] Rishi Bommasani and others, "On the Opportunities and Risks of Foundation Models" (arXiv, 12 July 2022) <http://arxiv.org/abs/2108.07258> accessed 21 May 2024.

[33] Art 3(65) AIA.

As far as prohibited practices high-risk AI systems and GPAI, the AIA assigns precise duties to AI providers,[34] the actors who develop AI systems, and deployers, the people who employ those AI systems,[35] depending on the risk generated by the AI system or model. Moreover, the AIA builds a complex transnational and EU governance system to govern the most impactful of those AI systems.[36] Some uncertainty is still present as far as the compliance rules to apply for AI systems not falling explicitly into the previously described systems. Specifically, I am referring especially to the category of "low-risk" AI systems which was present in the first 2021 AI proposal but was subsequently "forgotten" from the AIA negotiations and the introduction of GPAI[37] really stole the negotiations spotlight.

However, Article 4 AIA on AI literacy is a general, horizontal norm that applies to all kinds of AI systems and models and states several obligations that AI providers must be accountable for by instructing their staff and the AI system's affected people of the risks that their kind of AI might cause and which rights they do have if they sustain damage.[38]

2.2. *Product safety laws*

The second group of laws that manufacturers will need to deal with is the one concerning product safety. There will be three regulations to discuss, from the most general to the most specific.

The more general one is the recently approved General Product Safety Regulation (GPSR) which will become applicable from 13 December 2024.[39] It is important for mixed-functions IoT manufacturers as it considers as part of its applications field IoT objects – in its "product" definition[40] – as well as online marketplaces that sell them.[41] This new regulation is inspired by the administrative system created by the previous General Product Safety Directive (GPSD)[42] but includes some innovations, most notably a new recall system and the provision of traceability requirements for objects.[43] In sum, the manufacturers' common goal is to get the EU CE conformity label both under the GPSD and the GPSR. Moreover, in the GPSR there are complex and extended obligations falling on all the economic operators involved in the mixed-functions IoT objects production chain. This way of including all the economic operators involved is not exclusive of the GPSR but also of the Machinery Regulation (infra) and it started in the MDR which is the oldest and most

[34] Art 3(3) AIA.

[35] Art 3(4) AIA.

[36] Chapter VIII AIA.

[37] This category is inferred by the use of the "other-than high risk AI systems" expression by reading Art 69 of the AI proposal of 2021 on the obligation to adhere to codes Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS COM/2021/206 final.

[38] Arts 3(56) and 4 AIA read in combination with recitals 56,91 and 166 AIA. For the interpretation of Article 4 as a source of duties and obligations see also Irina Carnat "The cost of AI illiteracy," forthcoming 2024.

[39] Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC PE/79/2022/REV/1 [2023] OJ L 135/ 1.

[40] Art 3(1) GPSR.

[41] Art 3(13) GPSR as certain fulfilment services providers are online platforms, and 3(14) GPSR provider of an online marketplace.

[42] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety [2001] OJ L 11/ 4.

[43] Art 18 GPSR for the traceability obligations, and more specifically for the recall of dangerous products Arts 25–26 GPSR for the Safety Gate Rapid Alert System and Art 27 for the Safety Business Gateway that will enable online marketplaces and economic operators to provide information to market surveillance authorities and consumers at Art 27.

specialised of these regulations (infra). The rationale for having so many actors with duties is not to leave accountability gaps along the product and value chain and this is why the PLDU mirrors this scheme in Article 7 PLDU from a liability point of view (see 3.1). In fact, in the GPSR, manufacturers[44] have specific obligations such as the obligation to carry out a risk analysis of the marketed product.[45] Furthermore, the other economic operators have specific obligations such as authorized representatives,[46] importers,[47] and distributors[48] as well as online marketplaces.[49] Some rules shift manufacturers' obligations onto other economic operators in specific cases[50], in order not to leave accountability gaps. In addition, the application to IoTs in general, and to mixed-functions IoTs in particular, is highlighted in Article 6 GPSR which sets a non-exhaustive list concerning criteria on how to evaluate the safety of the product and explicitly mentions the effect that the product might have on other ones also because of their interconnection.[51]

The recent approval of the AIA act demonstrated what it had only been presumed during its negotiations: that there is a complementarity relationship between the AIA and the GPSR for the residual categories of the once called "low-risk AI systems"[52] and that is apparent by reading Recital 166 AIA. In the AIA, the only non-binding but explicit obligation is to draw codes of conduct inspired by the ethical principles of the High-Level Expert Group's "Ethical Guidelines for a trustworthy AI" principles for those kinds of algorithms.[53] The recently approved AIA confirms this as it uses the term "safety net" referring to the GPSR concerning other than high-risk AI systems which do not have a specific regime to follow. What would that mean in practice? It seems that the principles guiding the development non-high-risk AI systems will still be in the AIA[54], mainly in Article 4 on AI literacy and corresponding AI recitals as well as Article 70 AIA which concerns AI national authorities. However, for the safety and market surveillance obligations, AI systems providers (and, most likely mixed- functions IoT manufacturers) will need to consider the GPSR. Hence low-risk AI-powered mixed-functions IoT manufacturers will need to keep in mind this two-pronged system (AIA and GPSR) as far as compliance and accountability are concerned.

A more specific regulation in this group is the recently approved Machinery Regulation (MR) which can apply[55] to mixed functions IoT objects and their components if they are of the same kind as the ones of the list described in Article 2 and Annex II MR, including software as a safety component.[56] In addition to that, the MR rules applicable to mixed-functions IoT devices might also need to coordinate with Article 6 and Annex I (1) of the AIA. This AIA Article concerns high-risk AI systems which are either safety components or are AI systems covered by Annex I of the EU harmonization legislation and are required to undergo a third-party conformity assessment. The MR is part of those harmonization regulations contained in Annex I AIA. Reciprocally, Annex 2 (19) MR, mentions " . . . *Safety components with fully or partially self-evolving behaviour using machine*

[44] Art 9 GPSR.
[45] Art 9(1) GPSR.
[46] Art 10 GPSR.
[47] Art11 GPSR.
[48] Art 12 GPSR.
[49] Art 22, 27,34 for online marketplaces.
[50] Art 13 GPSR.
[51] Art 6(1)(b) GPSR.
[52] Recital 9 AIA, 166 AIA.
[53] Recital 165 AIA.
[54] Basically Art 4 AIA on AI literacy and the AI recitals with general character.
[55] Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC (Text with EEA relevance) PE/6/2023/REV/1 *OJ L 165, 29.6.2023, p. 1–102.*
[56] Annex 2(1) AIA.

learning approaches ensuring safety functions." In some specific cases, meaning when software is a safety component then, probably, the MR will need to be applied in conjunction with the AIA compliance discipline of high-risk AI systems if the software as a safety component falls within the parameters of Article 6 (1) and Annex I of the AIA. As for low-risk AI and the GPSR, it might be difficult to coordinate with the rather specific and complex MR discipline involving sometimes the same actors in the value chain.

Another element of similarity among these three legislations, including the MR, concerns the attribution of duties to economic operators: manufacturer, authorized representative, importer, and distributor.[57] Each of these subjects has its own duties, the most complex of which belong to the manufacturers who need to create the product which must respect the basic health and safety conformity requirements and send the necessary technical documentation which can undergo a third-party conformity assessment depending on the category and level of risk of the machinery.[58]

In 1.1, I explained that the manufacturer is the subject responsible for the certification strategy of their products, and they should do that by verifying the product safety rules that are applicable to their product. In case the manufacturer does not opt for the "general safety" laws as they believe the IoT object has medical functions and not only an e-health one, then the path to follow is the one set in the MDR. Even if the MDR field of application is specific and, regarding IoT objects, it only concerns medical IoT objects, which I will not analyse here, it also gives a little guidance concerning mixed-functions IoT objects. If one reads in conjunction Articles 2(2) and 2(11) MDR they come across the meaning of accessory of a medical device. More precisely, it can be a device or software (e.g. a smartwatch or a function for an integrated vocal assistant) which '. . . *whilst not being itself a medical device, is intended by its manufacturer to be used together with one or several particular medical device(s) to specifically enable the medical device(s) to be used in accordance with its/their intended purpose(s) or to specifically and directly assist the medical functionality of the medical device(s) in terms of its/their intended purpose(s).*'[59] If we want to expand even more the picture, Article 2(11) MDR explores the notion of system which is a combination of products, either packaged together or not, which are intended to be interconnected or combined to achieve a specific medical purpose. Nevertheless, the rigid distinction between medical and mixed-functions IoT still holds: Article 22(c) MDR provides that the other objects used in conjunction with one or more medical devices must bear a CE certification that is obtained through the processes described in the GPSD. This means that the GPSR will soon fulfil the GPSD role. Despite the MDR is not directly applicable to the mixed-functions IoT, it is important to point out that the MDR mentions non-medical devices used in conjunction with medical devices, such as software as a medical device, as it reinforces the hypothesis that in the near future medical IoT devices and mixed-functions IoT devices might work together although having a different regulatory discipline.

3. The maze part II: the liability regimes applicable to the mixed-functions IoT

In this section, I will briefly highlight the most relevant points concerning the application of the EU harmonized (or soon-to-be harmonized) liability rules to mixed-functions IoT devices. The objective of this section is to describe when either or both the AILDP and the PLDU will be applicable in the cases of damages created by mixed-functions IoT.

[57] See Arts 3 (18)–(21) MR.
[58] See Art 10–11 MR for a list of the manufacturer's major obligations.
[59] 2(2) MDR.

3.1. The new Product Liability Directive Update (PLDU) and the mixed-functions IoT

Concerning the first criteria of evaluation, the still applicable Product Liability Directive (PLD)[60] and PLDU (after its approval) might be the most relevant harmonized liability systems for the mixed-function IoT objects for several reasons. The first reason is that this kind of IoT devices are considered part of a larger consumer objects category under EU law, hence they will respond to this kind of liability even today when the PLD is still applicable. Moreover, as recalled in the explanatory memorandum for the PLDU, product liability is a gap filler for those EU legislative proposals and acts that might have a more decisive regulatory character the Machinery Regulation, and the General Product Safety Regulation.[61] In those acts, liability is not addressed. Hence, if damage occurs, the PLDU will be applicable. To sum up, the gap-filling function[62] will be the ultimate scope of EU product liability.

The process of the PLD review for the REFIT[63] review of the EU legal acts in 2018 crossed paths with the scholarly debate on the fitness of the PLD for the digital age.[64] In the end, the idea was to update the PLD with the consolidated Court of Justice of the EU (CJEU) jurisprudence and the changes brought by new digital technologies at the same time. That is why it is relevant to focus on the new PLD Update (PLDU) proposal which was made public last 28 September 2022 together with the AILP (infra 3.2).

The PLDU functioning is not completely different from the current PLD one as the complainant needs to prove the damage, the defectiveness, and the causal link between the first two elements.[65] However, the application of the new PLDU will be especially interesting for the mixed-function IoTs for several reasons. Firstly, it will be a general regime that has the role of covering the mixed-functions IoT, even when they are part of a medical device in the form of ancillary products or as part of a system of medical devices according to the MDR. At this moment, both medical devices and consumer IoTs need the PLDU application whenever the kind of damage covered by this directive proposal takes place. Secondly, what is interesting to notice is that the new PLDU proposal is similar to the MDR under a terminology aspect. For instance, the "producer" has disappeared and has been substituted by the "manufacturer."[66] Moreover, other terms such as economic operators, or authorized market representatives are more in line with the vocabulary of the MDR and the product safety laws (see sect. 2.3).

It is interesting to point out that the concept of a product (which can become defective) extends explicitly beyond the tangible part of the object. In fact, in Article 4(1) PLDU the definition of product comprehends software but also digital manufacturing files and components, the latter ones must be with the manufacturer's control, as well as the related services.[67] The PLDU describes these last elements by stressing their function of

[60] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products [1985] OJ L 210/29.

[61] PLDU explanatory memorandum, p.3–4.

[62] Norbert Reich, 'Product Liability and Beyond: An Exercise in Gap-Filling'; (2016) 24 European Review of Private Law <https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\ERPL\ERPL2016038.pdf> accessed 21 May 2024.

[63] European Commission, 'REFIT – making EU law simpler, less costly and future proof' (European Commission official website),<https://commission.europa.eu/law/law-making-process/evaluating-and-improving-existing-laws/refit-making-eu-law-simpler-less-costly-and-future-proof_en> accessed 21 May 2024.

[64] Christiane Wendehorst, "Strict Liability for AI and other Emerging Technologies" [2020] 11/2 Journal of European Tort Law <https://doi.org/10.1515/jetl-2020-0140> accessed 15 March 2024.Report on the liability of AI and emerging technologies; Giovanni Comandé 'Multilayered (Accountable) Liability for Artificial Intelligence'," in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds) *Liability for Artificial Intelligence and the Internet of Things. Münster Colloquia on EU Law and the Digital Economy* (Nomos Verlag- Hart Publishing, 2019) 165–183.

[65] Arts 2, 6, 9 PLDU.

[66] Art 1 PLDU.

[67] Art 4(4) PLDU.

integration and interconnection but also by pointing out that the lack of said services would prevent the product from performing one or more of its functions. Furthermore, for the first time, the definition of damage encompasses not only physical damage (including psychological damage) and physical property but also the loss or corruption of data.[68] This is likely to result in one of the most common damages that could be caused by using mixed-functions IoTs. It will be interesting to analyse how the different national judges will find a way to effectively measure the damage created by data loss according to their national laws and the interaction of data loss damage with damage reparation rules set in Article 82 GDPR.[69] The importance of data and software in general over the hardware part of products is also reflected by Article 10(2) PLDU on liability exemptions. Whenever software or its absence, or a related service caused the damage the manufacturer cannot state that the defect did not exist at the time of putting into the market the product or the service.

One of the most interesting elements of the PLDU concerns its relationship between standards and liability. As in the current PLD, and maybe symbolically, Article 6 PLDU deals with defectiveness. From the letter of the provision, it seems that the safety paradigm stays the same, but its point of reference changes: the "public at large" instead of what a person can reasonably expect. One could wonder what the public could exactly expect from a mixed-functions IoT device, which can also work in connection with one or more medical devices. The perceptions of risk and safety would likely change in all the possible applications of mixed-functions and medical IoT devices working together or alone. The defectiveness indicators list that follows in Article 6 PLDU is likely to be interpreted, as the one in current Article 6 PLD, as not a conclusive and final one.[70] What is important to notice is that Article 6(f) and (g) PLDU consider as one of the elements to evaluate defectiveness the non-compliance with product safety requirements, including safety-relevant cybersecurity requirements. This is essential given the space that is left to standards and common specifications not just in the MDR but also in the AIA and the product safety regulations. It is a good sign that the PLDU does not mention any of the regulations for cybersecurity, data-sharing, and safety. In fact, the contrary will most likely make the PLDU grow old before its time.

Moreover, it is necessary to highlight the importance of Article 8 PLDU on evidence disclosure and of Article 9 (2–5) PLDU concerning the defectiveness and causal link (rebuttable) presumptions. As in Articles 3 and 4 AILP, Articles 8 and 9 are PLDU are entwined, and they are the result of EU experts report about the impact that AI and new technologies have on liability.[71] Article 8 allows claimants to ask judges to require manufacturers to show how their product works on the condition that enough facts support this request for compensation. At the same time, the intellectual property rights of the manufacturer must be somehow protected. Article 9(2) sets three non-cumulative conditions to prove the defectiveness of the product which are the following: (i) the

[68] Art 4(6) PLDU.

[69] The CJEU implicitly gave some advice on how to interpret Art. 82 GDPR concerning the need for evidence of a prejudice whenever the GDPR was infringed. It could be that national judges decide for that too. See case C-300/21 *UI v Österreichische Post AG* ECLI:EU:C:2023:370.

[70] The criteria of Art 6(1) PLDU can all be interpreted in a more consumer-favorable way: (a) the presentation of the product; (b) the reasonably foreseeable misuse of the product; (c) the effect on the product of any ability to continue to learn after deployment; (d) the effect on the product of other products that can reasonably be expected to be used together with the product; (e) the moment in time when the product was placed on the market or put into service or, where the manufacturer retains control over the product after that moment, the moment in time when the product left the control of the manufacturer; product safety requirements, including safety-relevant cybersecurity requirements; any intervention by a regulatory authority or by an economic operator referred to in Art 7 relating to product safety; h) the expectations of the end users.

[71] Expert Group on Liability and New Technologies, *Liability for artificial intelligence and other emerging digital technologies* <https://op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en> accessed 21 May 2024.

defendant has failed to comply with Article 8 evidence disclosure obligation (ii) the claimant demonstrates that the product does not comply with mandatory safety requirements laid down in Union law or national law that are intended to protect against the risk of the damage that has occurred; (iii) or, the claimant demonstrates that the damage was caused by an obvious malfunction of the product during normal use or under ordinary circumstances. Article 9(3) introduces a rebuttable presumption by stating that if the damage is consistent with a certain cause a causal link can be presumed. Ultimately, the judge can freely decide, because of technical difficulties experienced by the complainant, to presume either/both the causal link or/and defectiveness provided that the complainant proves that the product contributed to the damage and it is likely that its defectiveness was likely to have caused the damage.[72] All these presumptions might be interpreted more in favour of consumers than one might expect, as judges might feel more sympathetic towards a consumer who does not know how a seemingly straightforward, but complex, mixed-function IoT device might work.

Despite these premises, the future enforceability of the PLDU could create problems for consumers. One of the underlying issues in Article 7 PLDU is the lack of flexibility in the liability regime applicable to the different economic operators involved in the production of technological products, such as the mixed-functions IoT objects. In theory, the directive's rationale is pro-consumer as the consumer must always have an EU-based subject they could address.[73] The problem is that the first subject the consumer needs to contact in case of damages is always the manufacturer which could also be not EU-based in case it is a technological object such as a mixed-functions IoT. That might often be the case for technological products. Besides, Article 7 PLDU provides for a strict subjects list (from the further one to the nearer one to the consumer) to ask for compensation. Such order is understandable under a regulatory perspective for accountability reasons but might discourage consumers from taking advantage of this kind of liability because of the length of this list, the time, the costs that it might entail and, finally, the risk of being time-barred.[74]

3.2. The proposed AI liability directive (AILDP)

In terms of liability schemes, mixed-function IoT devices could also be potentially subject to the proposed AI non-contractual liability directive. This is a fault-based liability directive although it does not harmonize the concept of fault directly. It does that by exemplifying breaches of duties of care when it comes to AI development and through legal presumptions concerning the causal link between the damage and the AI system's functioning.[75] It applies to mixed-functions IoT because the technologies concerned (the IoT and the AI) are already working – if not within the same physical device – at least in combination through sensors and cloud (mostly proprietary) networks. This way of operating is the same both for mixed-function IoT devices and for certified IoT medical devices.

[72] Art 9(4) PLDU.

[73] PLDU Explanatory memorandum p.2.

[74] Art 7 PLDU lists the following stakeholders: the manufacturer, the importer, the authorised representative and the fulfilment service provider, the refurbished/second hand seller, the distributor and the online platform. On a different note, the CJEU with the *Fennia* judgment established that whoever appears to be the producer needs to bear the possibility to receive claim for damages. Unfortunately, Art 3(3) PLD has not been maintained in Art 4 and 7 PLDU. Therefore, it is uncertain that this interpretation could hold when the PLDU enters into force. Case C-264/21 *Keskinäinen Vakuutusyhtiö Fennia v Koninklijke Philips NV*. ECLI:EU:C:2022:536. See Francesca Gennari, "A tale of two cities? Fennia v Philips and Article 7 of the Product Liability Directive Update" *EuCML* 12, (2023) :267–74.

[75] Arts 3 and 4 AILDP.

The AILDP will respond to non-contractual kind of claims caused by AI. Given that the damage from software needs to be considered also as falling within the PLDU regime[76], the AILDP will cover only the claims in which damage is caused by software that:

(i) could be defined as AI system by the new text of the AIA and
(ii) injures, in a material and non-material way depending on the tort national rules, a party not involved in the AI system creation and deployment which I will generally refer to here as third party.

For instance, I use a visor with augmented reality to do rehabilitation, but the object is an IoT which is not certified as a medical device. However, this visor works in collaboration with the hospital and in this way, the doctor knows that I am doing physical exercise at a number of times per day. A friend comes to my place and tries on the visor. The problem is that the virtual reality landscape they see is incorrect. Hence, they jump from the sofa, and they break their ankle. Leaving aside for the moment my responsibility in leaving that object unattended, the friend could sue the IoT manufacturer (which could also be the AI provider) by using the national implementation of the AILDP. In this case case, the national rules concerning general non-contractual liability will be harmonized with the presumptions contained in Article 4 AILDP and the new procedural rules concerning evidence disclosure in Article 3 AILDP.

Article 4 AILDP is particularly interesting as three conditions must be satisfied by the claimant for the national courts to presume a causal link. The first one is to prove the fault of the defendant, the second one is that it must considered likely that the defendant's fault was the cause of the AI-induced damage, and the third one is to demonstrate that the output produced by the AI system or the failure of the AI system to produce an output gave rise to the damage.[77] However, if the system is high-risk according to the AIA, the first condition could be presumed if the claimant manages to prove at least one of the breaches of duty of care set in Article 4(2). These duties concern, among others, duties of transparency and fairness of data training to make just two examples. However, this will not apply when the defendant proves that the state of the art makes it possible to prove causality without using Article 4(1) AILDP presumptions for high-risk AI systems.[78]

This analysis of the AILDP suffers from the interconnection of this legislation with the AIA first proposal and might be subject to changes quite soon. When the AILDP proposal was presented, it referred to a version of the AI act that is quite different from the one that was approved recently. Hence, this analysis might become outdated too in a short time. There is no mention of GPAIs in the AILDP and one can ask if they can be assimilated to high-risk AI systems in terms of AILDP presumptions especially if we consider GPAI with systemic risk or that have an opaque way of functioning and AI deployers/implementers do not know how to mitigate risks which might injure an undetermined but high number of people.

Even if we consider that the AILDP will not change (or change much) from the text that we are discussing today, I think that its application might be residual even for the national judges' law practice, specifically for AI systems that correspond to the old "low-risk" AI systems and which fall in the general Article 4(1) AILDP scheme. These low-risk AI systems are relevant as they are most systems that power mixed-IoT objects today. One problem for the complainant's lawyers could be the following: for most of them, it will be difficult to

[76] Art 4(1) PLDU. The overlap concerning software and AI between the two directives is described in depth in Gerhard Wagner, "Liability Rules for the Digital Age: – Aiming for the Brussels Effect –" (2022) 13 Journal of European Tort Law 229–30.

[77] Art 4(1) AILDP.

[78] Art 4(4) AILDP.

demonstrate that there is no other way to prove causation than to use Article 3 AILDP and gain access to how the algorithms work. Nevertheless, lawyers do not have the skills to understand how AI works, unless serious training is organized. But, even with training, it will be complex to find expert AI consultants in the short run. However, a more complainant friendly way to interpret Article 4(1) is through Article 4(5) which states that for low-risk AI systems judges can "*only apply where the national court considers it excessively difficult for the claimant to prove the causal link mentioned in paragraph 1*." This cannot work if the complainant uses the mixed-functions IoT is for a personal or nonprofessional activity according to Article 4(6) AILDP.

Even if the complainant's lawyer manages to prove through Article 3 AILDP the condition set at Article 4(1)(a), there are still other two conditions to prove together with the fault of the AI provider. In sum, the new harmonized general tort rules might not be as favourable to injured people as one might think they are. A liability system indeed needs to strike a balance between the different actors involved. However, in this case, it seems too tilted in favour of AI providers/manufacturers. They are the subjects that do know best how AI systems work.

What is going to be likely is that for mixed-IoT objects, if the AILDP needs to be applied, is that national judges will try to interpret the AILDP provisions more favourably towards the injured party, especially if the AI system is complex, independently from the level of risk and maybe by taking inspiration by Article 9 PLDU presumptions and/or by adding national implementation rules on the matter. This would follow the interpretation of Article 1(4) AILDP which allows Member States to adopt or maintain national rules that are more favourable towards injured people if they are compatible with EU law. It seems that only Recital 14 AILDP suggests that this directive should be interpreted as a minimum harmonization directive, but this indication is not present in the main text. This poses serious concerns because what would be the rationale of having a minimum harmonization directive for AI non-contractual liability if every member state can create EU law-compliant and yet more complainant-friendly AI tort rules when this proposal's legal basis wants to avoid excessive market and legal fragmentation?

If there will be a change following the AIA approval in the AILDP structure, it will be a good occasion also to clarify this last point concerning a clearer division between the EU and national liability regimes, and making it explicit that it is a minimum harmonization directive, as well as whether or not to include presumptions for GPAI models and systems.

4. Preliminary conclusions

The mixed-functions IoT devices are an increasingly important kind of connected objects that will become crucial in the next years. They will likely become the main facilitators between a more connected home and the need for rehabilitation or exercise for an increasingly old, but more digitally literate, population of users in a post-COVID-19 pandemic world.

According to the definition of mixed-functions IoTs as objects that are consumer objects but that could integrate an e-health function and connect to other more specialised medical devices in the vicinities or at a distance, several legislative and prospective EU acts may apply. My focus was tort liability rules, and the most relevant regulatory safety frameworks for mixed-functions IoTs upon two considerations: the need to find a *fil rouge* within the current regulatory framework that applies to these devices, and the consequences on the interactions among different legislations when applied to cases involving future mixed-functions IoT.

The most relevant conclusions for mixed-functions IoT objects are the following. One concerns the coordination between overlapping risk management systems concerning

safety and AI. The other one concerns the liability rules which depend on the clarification of said risk-management duties.

As far as the coordination aspect is concerned, the safety legislations with the AIA are going to be used at the same time, both in the case of high-risk and low-risk AI systems. In case of high-risk AI systems working in the mixed-functions IoT, the AIA needs to be coordinated with the MR. In the case of low-risk AI systems which will most likely concern the majority of mixed-functions IoT, the AIA literacy principle will need to be coordinated with the GPSR. This justifies a clarification on how to best coordinate and harmonize the AIA with these other regulations for manufacturers and the other economic operators involved to also understand the extent of the duties of care for possible liability claims.

As far as liability, the PLDU will be the main liability regime applicable to the mixed-functions IoT objects in case material or non-material damage arises, and the subject involved is a consumer. The defectiveness indicators as well as the presumptions concerning causality seem to help the consumer more than with the AILDP regime, which could probably remain a residual set of rules in practice. However, as far as the PLDU is concerned, it is still uncertain whether the complex structure of Article 7 PLDU, concerning the identity of the manufacturer, will be easily applicable to the mixed-functions IoT devices. Despite mixed-functions IoT might seem simple objects, they might have complex product and value chains.

The AILDP instead will most probably need modifications as it takes as a reference the AIA proposal and not the approved AIA. For instance, there is no mention of GPAI therefore it is likely to think that it might change soon. As it is now, the AILP could be used mainly in cases where a third party has been injured by the AI system working in the mixed-functions IoT object. It seems that a more complainant-friendly interpretation in applying the presumption of Article 4(1) depends on whether the judges find it excessively difficult for the complainant to prove the causal link when it comes to low-risk AI systems. Moreover, an AILP update is also requested to understand whether it is minimum harmonization directive also in its main text and, if that is the case, make the AILDP presumptions more clearly in favour of complainants. If MS can enact more favourable rules, then, what is the point of an AI liability harmonization at all if the EU regime is not more favourable to claimants?

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

I would like to thank the anonymous reviewers for their time and care in reviewing my manuscript. I warmly thank Professor Giovanni Comandé, Professor Federica Casarosa and Ms. Irina Carnat, research fellow, for their insights and suggestions.

Competing interests. The author declares having no conflict of interest.

Cite this article: F Gennari (2024). "Mixed-Functions IoT devices: a Regulatory and Liability Requirements' Maze. A First Overview". *European Journal of Risk Regulation* **15**, 912–927. https://doi.org/10.1017/err.2024.68