Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots

Eduard Fosch-Villaronga[a,*], *Tobias Mahler*[b]

[a] *eLaw Center for Law and Digital Technologies, Leiden University, Leiden, the Netherlands*
[b] *Norwegian Research Center for Computers and Law, University of Oslo, Oslo, Norway*

ARTICLE INFO

Keywords:
Cybersecurity
Safety
Robots
Human–robot interaction
Connected products
Medical Devices
Healthcare
GDPR
NIS Directive
Product Safety

ABSTRACT

This paper addresses the interplay between robots, cybersecurity, and safety from a European legal perspective, a topic under-explored by current technical and legal literature. The legal framework, together with technical standards, is a necessary parameter for the production and deployment of robots. However, European law does not regulate robots as such, and there exist multiple and overlapping legal requirements focusing on specific contexts, such as product safety and medical devices. Besides, the recently enacted European Cybersecurity Act establishes a cybersecurity certification framework, which could be used to define cybersecurity requirements for robots, although concrete cyber-physical implementation requirements are not yet prescribed. In this article, we illustrate cybersecurity challenges and their subsequent safety implications with the concrete example of care robots. These robots interact in close, direct contact with children, elderly, and persons with disabilities, and a malfunctioning or cybersecurity threat may affect the health and well-being of these people. Moreover, care robots may process vast amounts of data, including health and behavioral data, which are especially sensitive in the healthcare domain. Security vulnerabilities in robots thus raise significant concerns, not only for manufacturers and programmers, but also for those who interact with them, especially in sensitive applications such as healthcare. While the latest European policymaking efforts on robot regulation acknowledge the importance of cybersecurity, many details, and their impact on user safety have not yet been addressed in depth. Our contribution aims to answer the question whether the current European legal framework is prepared to address cyber and physical risks from care robots and ensure safe human–robot interactions in such a sensitive context. Cybersecurity and physical product safety legal requirements are governed separately in a dual regulatory framework, presenting a challenge in governing uniformly and adequately cyber-physical systems such as care robots. We conceptualize and discuss the challenges of regulating cyber-physical systems' security with the current dual framework, particularly the lack of

* Corresponding author: Eduard Fosch-Villaronga, eLaw Center for Law and Digital Technologies, Leiden University, Steenschuur 25, 2311 ES Leiden, the Netherlands.
E-mail addresses: e.fosch.villaronga@law.leidenuniv.nl (E. Fosch-Villaronga), tobias.mahler@jus.uio.no (T. Mahler).

https://doi.org/10.1016/j.clsr.2021.105528

mandatory certifications. We conclude that policymakers need to consider cybersecurity as an indissociable aspect of safety to ensure robots are truly safe to use.

1. Introduction

Robots are cyber-physical systems that combine hardware and software components, network and communication processes, mechanical actuators, controllers, operating systems, and sensors to interact with the physical world (Quarta et al., 2017). Typically divided between industrial and service robots depending on whether they are 'for use in industrial automation applications' or 'perform useful tasks for humans' (ISO 8373 2012), these complex systems increasingly interact with humans in professional, public, private, or healthcare settings. Examples include industrial robots, warehouse robots, feeding robots, exoskeletons, assistants, socially interactive robots, robotic wheelchairs, or robotic surgeons. The characteristic feature of these systems is that they create an interconnected structure where the virtual and the physical intersect (Fosch-Villaronga and Millard, 2019).

Cloud services allow robots to offload heavy computational tasks such as navigation, speech, or object recognition on the cloud, and mitigate this way some of the limitations posed by their physical embodiment (Fosch-Villaronga and Millard, 2019). However, 'the more functions are performed across interconnected systems and devices, the more opportunities for weaknesses in those systems to arise, and the higher the risk of system failures or malicious attacks' (Michels and Walden, 2018). To date, nonetheless, there is little understanding to what extent an attacker can exploit the computational parts of a robot to affect the physical environment in industrial (Quarta et al., 2017), social (Lera et al., 2017), or medical environments (Bonaci et al., 2015), and what that would entail for the users involved in the interaction.

Some authors argue that while robotics manufacturers set a high priority on safety, development costs, market timing, and customer-oriented features; consumers often disregard security concerns, valuing more usability, functionality, and competitive prices (Clark et al., 2017). However, research indicates consumers' willingness to prioritize and pay more for higher security when they buy connected products, provided the security level is communicated in a comprehensible way, such as a security label (Johnson et al., 2020; European Commission, 2020a, 2020b).

Furthermore, security vulnerabilities in robots raise significant concerns for manufacturers, programmers, and for those who interact with them in domains of sensitive applications such as healthcare. In a healthcare setting, robots interact in close, direct contact with children, older adults, and persons with disabilities and it may be unclear for the target user whether the robot is functioning properly or is under attack (Fosch-Villaronga et al., 2018). Attackers can compromise the controlling of robots and have effects on the production chain (Quarta et al., 2017). In the health sector, such an attack to a healthcare robot may affect the health, well-being and safety of people, something that agencies like the Food and Drug Administration (FDA) in the U.S. identify as an unresolved, major concern (FDA, 2019).

Interconnected 'things' and robots outside of factories are relatively new, and legislation establishing safety requirements was mostly designed for things working in isolation, mostly in industrial environments. Revisions of these legislations, mainly the General Product Safety Directive, are only scheduled for this year 2020.[1] Cybersecurity and safety concerns are also often addressed in separate pieces of legislation, as if policymakers failed to recognize the link between cybersecurity and safety in the case of cyber-physical systems, including products, or medical devices (FDA, 2019).

In this paper, we argue that, as cyber-physical systems, robots need safeguards relating to the physical and digital parts to be safe. Robots represent an interface to the physical world, making security concerns particularly salient because, unlike traditional computers, they can have an immediate physical effect on their environment (Morante et al., 2015). Acknowledging such a link is essential in the healthcare domain, as 'vulnerabilities could allow unauthorised users to remotely access, control, and issue commands to compromised devices, potentially leading to patient harm' (FDA, 2019).

Our contribution aims to highlight the missing link between cybersecurity and safety and to discuss potential solutions within the current European legal framework. Cybersecurity and physical product safety legal requirements are governed separately, presenting a challenge in governing uniformly and adequately cyber-physical systems such as care robots. We conceptualize and discuss the challenges of regulating cyber-physical systems' security with the current weak link between safety and cybersecurity, particularly the lack of mandatory professional certifications. We cover an area, care robots, where cybersecurity and its impacts on user safety are particularly salient.

2. Cybersecurity, safety, and robots

Cyber-physical systems may present a risk in case of cyberattacks. In 2015, a Jeep Cherokee was switched off remotely by hackers while being driven by a journalist.[2] In another example, the Stuxnet virus subtly changed the speeds that the

[1] The European Commission has appointed several experts to advise the Consumer Safety Network (CSN) in the revision of the General Product Safety Directive under the 'Sub-Group on Artificial Intelligence (AI), connected products and other new challenges in product safety.'

[2] *See* https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ and https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/?event=viewProduct&reference=A12/1671/15&lng=en.

Iranian nuclear centrifuges spun, damaging or destroying the carefully calibrated machines (Holloway, 2015). These are examples that highlight the very real risks of exploiting the vulnerabilities of cyber-physical systems in general.

These cybersecurity risks are also relevant for the context of service robots, because systems that exert direct control over the world can cause harm in a way that humans cannot necessarily correct or oversee (Amodei et al., 2016). Service robots interact with humans and, in the healthcare sector, users are often in a vulnerable position, which makes these risks more critical. For example, a teleoperated surgical robot has been hacked by researchers, and bodily harm might have been the consequence, if this had been done by a malicious hacker.[3]

In this article, care robots are used as an illustrative example of a cyber-physical system that interacts with vulnerable parts of the population. Vulnerabilities in such examples are particularly salient because hackers could remotely access, control, and issue commands to compromise the robot, potentially leading to patient harm.

2.1. *Care robots as human-interacting machines*

There is an increasing policy interest in transforming healthcare in a way comparable to how robotics changed the industry in terms of increased productivity and resource efficiency (Cresswell et al., 2018). The urge to increase the quality and safety of care while simultaneously restraining expenditure motivates such policy interest (Yang et al., 2017). To this end, healthcare robots are likely to be deployed at an unprecedented rate (Simshaw et al., 2015) as a result of their reduced cost and their increased roles and capacities ((COMEST, 2017) to perform medical interventions, support impaired patients, provide therapy to children or keep the elderly company (Fosch-Villaronga and Drukarch, 2021).

In 2019, the Policy Department for Economic, Scientific and Quality of Life Policies of the European Parliament identified robotic surgery, care and socially assistive robots, rehabilitation systems, and training for healthcare workers as 'the most interesting applications of healthcare robots' (Dolic et al., 2019) (Table 1):

The European Parliament also highlighted that 'possible applications of AI and robotics in medical care (*are*) managing medical records and data, performing repetitive jobs (analyzing tests, X-rays, CT scans, data entry), treatment design, digital consultation (such as medical consultation based on personal medical history and common medical knowledge), virtual nurses, medication management, drug creation, precision medicine (as genetics and genomics look for mutations and links to disease from the information in DNA), health monitoring and healthcare system analysis, among other applications' (European Parliament, 2019).[4] These applications are mainly software-based Artificial Intelligent (AI)-driven technologies, that may be embodied or not.

Table 1 – Examples of 'most interesting' healthcare robot applications according to the Policy Department for Economic, Scientific and Quality of Life Policies of the European Parliament (Dolic et al., 2019).

Healthcare robot applications	
Robotic surgery	Allowing more accurate, less invasive and remote interventions relying on the availability and assessment of vast amounts of data
Care and socially assistive robots	Allowing to meet the expanding demands for long-term care from an aging population affected by multi-morbidities
Rehabilitation systems	Supporting the recovery of patients as well as their long-term treatment at home rather than at a healthcare facility
Training for health and care workers	Offering support for continuous training and life-long learning initiatives

The European Foresight Monitoring Network (EFMN, 2008) defined healthcare robots as systems able to perform coordinated mechatronic actions (force or movement exertions) based on processing information acquired through sensor technology, to support the functioning of impaired individuals, medical interventions, care and rehabilitation of patients and also individuals in prevention programs.

Some robots depend mainly on their physical embodiment because they need to perform a task that affects their immediate environment, for instance, to deliver medicines in a hospital, pick up an object from the floor or help patients get dressed. Others, on the contrary, may have a greater reliance on cloud services, for example, if an intelligent speaker hears and answers a question from a user in real-time and in natural language (Fosch-Villaronga and Millard, 2019). As Amodei et al. (2016) explain, systems outputting a suggestion to human users, such as speech-based systems, may have relatively limited potential to cause physical harm compared to those systems that exert direct control over the physical world. Still, these systems could challenge the mental health and the emotional wellbeing of users too. Cybersecurity-related incidents may then manifest in various degrees for users, depending on the type of attack but also on the configuration of the robotic system and it is essential to have an holistic understanding of *safety* in this respect.

2.2. *Care robots' cybersecurity*

Care robots' cybersecurity is underexplored in the literature. We conducted a literature review of relevant technical articles, mainly derived from searches at the IEEE or the arXiv databases. For the arXiv database from Cornell University, the words "healthcare robot cybersecurity," produced no results,[5] while the words "medical robot cyber security" pro-

[3] MIT Technology Review, Security Experts Hack Teleoperated Surgical Robot, April 24, 2015, https://www.technologyreview.com/2015/04/24/168339/security-experts-hack-teleoperated-surgical-robot/.

[4] Italics added.

[5] *See* https://drive.google.com/file/d/1rVtW1M2uRMHiQUHR7-kNT_L3yfOz7A_Ia/view?usp=sharing, captured on October 10, 2019.

Table 2 – Example of a care robot security attack based on (Clark et al., 2017).

Attack scenario for care robots
Consider the use of a robot in the home of an elderly person that lives alone. The function of the robot would be to allow the user's family to remotely monitor and locate him/her in case of a medical or health crisis. The robot is connected to the Internet via the home's wireless network and is equipped with a video camera, microphone, and speaker for the family to both view and communicate with the user. A financially motivated attacker could perform an application level attack by penetrating the home network and probing for the robot's IP address to reach the username/password login entry. Using a buffer overflow attack the attacker uses the entry of the login to overflow the stack with malicious code and inserts a return address that points to the malicious code. Once executed the attacker could have full control of the robot and is then free to monitor the elderly victim via camera or microphone seeking out information such as credit card data to be used for financial gain.

Table 3 – Modeling the robot cybersecurity scenarios (Lera et al., 2017).

Modeling the robot cybersecurity scenarios		
Origin	Accidental, unforeseen	
	Natural, natural disasters	
	Attack, generated by external users	
Target	Physical	
	Cyber	
	Cyber-physical	
Robot impact	Destruction, non-operability	
	Partial damage, robot malfunction	
	Degradation, capability decreased over time	
	Disruption, interruption	
	Unexpected behavior	
External impact	Public and private regulation entities	Final user
		Business
		High-level organization
Risk	Safety	
	Privacy	
	Confidentiality	
	Integrity	
	Availability	

duced only three results.[6] For IEEE Xplore Digital Library, 15 results appeared after including ("All Metadata": healthcare OR "All Metadata":care) AND ("All Metadata": robot OR "All Metadata": robots) AND ("All Metadata":cyber security OR "All Metadata":cybersecurity). The words "healthcare robot cyber security," produced eight results,[7] of which one is a table of contents, another is a review of the conference IEEE PerCom 2015, a previous paper on cloud services for healthcare robots (Fosch-Villaronga et al., 2018). The rest focused on mobile health applications, 'smart healthcare devices,' or in general on cyber-physical systems but did not have a clear focus on the researched topic. Although the search "medical AND robot AND cyber AND security" in the IEEE database produced 22 results, the majority of them did not relate to healthcare applications, or they were tables of contents which did not help our content gathering.[8] Based on these results, we handpicked articles that corresponded to similar keywords in Google scholar, focusing on existing literature on industrial robots, and without following any systematic approach.

Part of the available technical research has examined cybersecurity vulnerabilities in industrial production lines (Quarta et al., 2017) and telerobotic surgery (Bonaci et al., 2015). However, there is still little understanding of the actual risks of attacks exploiting security vulnerabilities of other robots in healthcare, such as exoskeletons, companion robots, or socially assistive robots (Ayala, 2016).

The following example relates to care robots (Table 2):

This example illustrates one plausible negative outcome that an attack on a care robot could involve, but we could think of other scenarios involving surgery robots, physically assistive robots such as lower-limb exoskeletons, or social robots for dementia or autism and the consequences an attack would imply for the user. To understand the underlying magnitude of the problem, we bring forward findings concerning robot security for medical robots as exposed in the work of Lera et al. (2017) who modeled the security scenarios depending on their origin, the target, the robot impact, the external impact, and the risk (in their case, privacy and safety) (Table 3):

This classification complements the description of Clark et al. (2017), who categorized embedded systems cyberattacks in hardware, firmware, and application. Hardware attacks may happen during the production time or the robot use, and typically include hardware backdoors, hardware trojans, eavesdropping, fault injection, and hardware modification (Clark et al., 2017). At the application level, typical attacks include viruses, worms, software trojans, and buffer overflow (Clark et al., 2017). In the example above, a buffer overflow attack allows an attacker to have full control of the robot, which could subsequently compromise the private information of the user, but also affect his or her safety.

The attacks may look different if the robot is autonomous or teleoperated, and various embodiments of robots, including highly anthropomorphic robots or wearable robots, can open specific risks (Fosch-Villaronga, 2019a). Bonaci et al. (2015) report that specific attacks are very noticeable in teleoperated robotic surgical systems. For instance, intention modification attacks involve unusual robot movements, which the surgeon can easily observe because he or she knows what to expect from the system. Other attacks like intention manipulation, however, are much harder to notice (Cerrudo and Apa, 2017). In these attacks, the attacker only modifies feedback messages originating from a robot. If the surgeon assumes the feedback of the surgical robot as valid, then he or she will act upon it and may unintentionally harm a patient (Wedmid, Llukani and Lee, 2011). Unfortunately, the noticeability of the attack may

[6] *See* https://drive.google.com/file/d/1Gi7xuDdUIRrsH2eWeKm-1oIK4tFsVEjzs/view?usp=sharing, captured on October 10, 2019.

[7] *See* https://drive.google.com/file/d/1Ear4nT8wAfCscyxgeep_omiRGAN76FYO/view?usp=sharing, captured on October 10, 2019.

[8] *See* https://drive.google.com/file/d/1cy29fkL1fRcw1nIUDMpG-9VI0rsuKkDle/view?usp=sharing, captured on October 10, 2019.

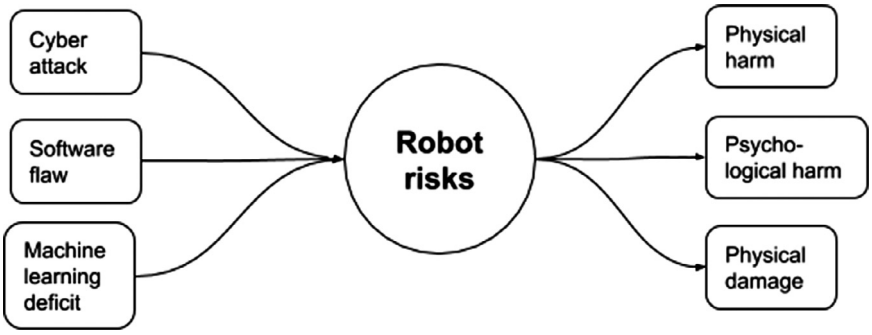

Fig. 1 – Robot risk bow-tie diagram: various cyber risks may lead to consequences in the physical context in which the robot operates.

not be evident for patients and inexperienced users that do not know what the expected behavior of the robot is. This could happen with social robots supporting elderly or children. Robot users may not notice that the robot is not the only relevant unit in the interaction but that many information flows happen in the background (Fosch-Villaronga et al., 2018). In this sense, malfunctions or modifications in the robot's behavior may equally remain unnoticed as they may consider that behavior as a normal robot behavior.

Fig. 1 simplifies what we expounded before in a bow-tie diagram that illustrates how the cyber and the physical domains are connected in the context of robot risks, where risks can originate in the cyber-domain and can lead to physical consequences, including human physical and psychological harm. From this review, we see that there are cyber attacks that could potentially affect robot task performance and endanger users' safety, although it may not always be intelligible to the user.

These concerns show a clear link between cybersecurity and safety. The European Parliament has highlighted the importance of the security of robotic systems in several resolutions (European Parliament, 2017; European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics (2018/2088(INI)) 2018). Nevertheless, it is unclear what regulatory measures need to be taken as there may not be an urgent need to regulate *ex novo*, as there is already a body of laws in place that addresses some of these issues.

2.3. *The legal framework for care robots*

There is not a single, unified legal framework for the problems arising from human–robot interactions (Holder et al., 2016) let alone for healthcare robots (Fosch-Villaronga, 2019a). However, it is often unclear how such robots can be legally classified. Such classification depends on their intended use, so these robots could be seen as either *medical devices* or general *products*, which are regulated differently. Power dynamics between private standards and public policymaking, however, confuse robot classification and their subsequent governance further (Fosch-Villaronga and Golia, 2019a; Fosch-Villaronga and Golia, 2019b). While public policymakers understand *healthcare robots* as medical devices, the industry pushes for new 'in-between' categories such as *personal care robots* that are not medical devices although they are intended for care purposes (Fosch-Villaronga, 2016, 2019a). The ISO 13482:2014 standard on safety requirements for 'personal care robots,' for instance, defines this category as 'service robot that performs actions contributing directly towards improvement in the quality of life of humans, excluding medical applications.' The standard does not define *personal care*, although it excludes robots with medical purposes, and includes physical assistants such as exoskeletons, 'wheeled passenger carriers' reminding of wheelchairs (currently considered medical devices), and 'mobile servant robots' that may work as socially assistive robots in healthcare settings (Fosch-Villaronga, 2016, 2019a, 2019b).

These confusions blur the understanding of how healthcare robots are classified *legally speaking* and, subsequently, which requirements roboticists have to meet to be compliant with binding regulations. In turn, this ultimately affects their safety, as it is not clear what minimum safeguard baseline needs to be, by law, respected by robot makers. Although the industry took a step forward in regulating service robots outside the industrial context, this hidden confusion, in turn, opens the door to potentially noncompliant robots with existing binding regulations, such as the medical device regulation or the product safety directive. Industrial standards are nonbinding, with no fixed consequences for violations, and they cost money, representing the privatization of the law (Fosch-Villaronga and Golia, 2019a, 2019b). They also often focus on one single impact, namely physical safety, conveying the impression that other aspects such as privacy, data protection, autonomy, psychological harms, or dignity do not play a role in ensuring a *safe* human–robot interaction (Holder et al., 2016; Leenes et al., 2017; Fosch-Villaronga, 2019a). Moreover, words such as 'cyber' and 'security' do not appear in ISO 13482:2014 on safety requirements for personal care robots, and it is only very recently that medical devices have to incorporate cybersecurity requirements as established in Annex I of the new Medical Device Regulation (Medical Device Coordination Group, 2019).

Whether something is classified as a medical device, as an object of personal care, or a toy may vary depending on the intended purpose of the 'device,' which has several consequences for regulatory requirements. In this respect, it is worth reminding that what will count as a *medical device* is the real intended purpose of the device, not what the producer

states.[9] Important to mention also the lex specialis relationship between the product safety frameworks for the situations when they overlap (e.g. the consequences of a product being both a medical device, a toy and a (wired or wirelessly) connected product.

Although cyber-physical systems have existed for some time now, coupling material things with the Internet is quite recent. Robots combine computational and physical components, and, thus, both software-related and hardware-focused rules apply. First, the safety of the robot is regulated via different legislations covering various classes of products, such as those devices for intended medical purposes (i.e., medical devices), machinery, and toys. In addition, the regulatory framework for cybersecurity applies.

3. The legal frameworks ensuring safety and cybersecurity

Robots are data-driven technologies and a cyberattack may compromise the adequacy of the robot's operation and the users' safety. For instance, robot surgeons powering down mid-operation could endanger the success of the procedure (Alemzadeh et al., 2016); or lower-limb exoskeletons processing data erroneously could make users fall. Robots can inflict bodily harm either because of a technical malfunction, or due to a cyberattack, but this insight is only partly accounted for in the EU general product safety legislation. For example, the EU medical device regulation focuses in detail on safety, while it addresses cybersecurity briefly.

In this section, we discuss the link between the safety regulation of physical products and their cybersecurity. For that, we bring to the fore different pieces of legislation in the two regulatory frameworks. In the safety context, these are general product safety, medical devices, and radio equipment; while the NIS Directive (Directive (EU) 2016) and EU Cybersecurity Act are part of the cybersecurity framework.

3.1. *Safety regulation for products*

In the EU, a variety of safety requirements apply to product types such as toys, radio equipment, medical devices, and products in general, to ensure that only safe products are on the market. Most of these laws and technical standards reflect a moment in time when products did not interconnect with other devices or their environment. With the growing interconnectivity and the deployment of the Internet of Things (IoT), this panorama has changed. Today, attackers can hack many products for various reasons, representing a potential security threat. European consumer organizations have criticized the prevailing safety concept in product legislation as *completely outdated* because it does not cover security risks arising from the product connectivity and the potential hacking risk they have (Giovanni and Silva, 2018). On the other hand, some safety rules, such as the recently updated Medical Device Regulation (MDR) 2017/745 and the Radio Equipment Directive, include specific cybersecurity requirements, as further discussed below.

The applicability of these safety rules to care robots depends on their classification according to product categories. Are they intended for medical purposes and thus potentially count as medical devices? Can they qualify as toys? Do they contain wireless (radio wave) connectivity and are thus under the scope of the radio equipment legislation? The answers to these questions are too context-dependent for this paper, but the questions themselves serve to illustrate the siloed-thinking behind the European fragmented regulatory approach. The EU still calls these directives 'new approach', even though they were conceived in the 80s (European Commission, 2016).

3.1.1. *Product safety*

Robots may be regulated as *products* under the General Product Safety Directive (Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety 2001) and Directive 85/374/EEC on liability for defective products. Product liability rules primarily offer an *ex post* compensation mechanism, but indirectly they also provide incentives for manufacturers to improve, *ex ante,* the safety and security of their products, in order to avoid liability risks.[10] The applicability of product liability laws is not straightforward in the context of physically embodied robots comprising cyber-physical systems as 'product interconnected with services, (…) an inseparable mixture of hardware, software, and service' (Fosch-Villaronga and Millard, 2019).

These challenges also apply to the product safety legislation, which has a clear *ex-ante* focus. According to the General Product Safety Directive 2001/95/EC, only safe products should be on the market. Unfortunately, cybersecurity does not appear along with the text, nor even on art. 2.b) where safety is defined. The legal definition of safe products is quite broad and it can be understood as covering all kinds of risks that can, directly or indirectly, cause harm to consumers.

Traditionally, the definition has been interpreted to apply to risks that have a physical impact on the safety of persons, such as among others mechanical or chemical risks. An extended concept of safety encompasses protection against all kinds of risks arising from the product, including cyber-risks (European Commission, 2020c). However, it is unclear whether national agencies engaging in market surveillance and enforcement are sufficiently open to such a broad interpretation, so further clarifications may be useful. Moreover, the product safety framework includes software integrated in a product at the time of placing it on the market, but it is not clear whether updates thereof are included (ibid.), particularly when these add new features to the product.

Safety is challenged not because of interconnectivity or other elements *per se* but for the new harms and risks arising from the new elements of robots present:

- *Interconnectivity*: New technologies bring in a new dimension that goes beyond the personal and individual sphere:

[9] For more information, *see* the judgment of the court for the case C-329/16 Snitem and Philips France: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62016CJ0329&from=EN.

[10] On the liability issues of new technologies see further Expert Group on Liability and New Technologies (2019).

the possibility to do large-scale attacks at no-cost in real-time.

- *Products with interconnected services*: Rise of products with interconnected services via cloud computing, including cloud services. The availability of services is critical for ensuring the safety of the product. As examples, Google Home and Alexa are products with services (e.g., speech recognition) and physical presence, but which lack the capability to physically interact with their environment.
- *Greater ecosystem and supply-chain:* There is an increased number of entities behind the creation of a product, and it is important to think about holistic risks. More and more stakeholders and providers are providing services in conjunction with other stakeholders and the bearer of responsibility is blurring.
- *Cyber-physical nature:* Products increasingly incorporate cyber elements, including software and connected services. Cyber-physical products include possible risk transfers between physical and cyber elements (*see* Fig. 2).
- *Processing personal and non-personal (meta)data:* expanding (over)use of data processing for the functioning of products. Unforeseen uses of data (Cambridge Analytica case), potential privacy violations or discriminatory consequences arising from inadequate training data. Increased attention to the link between processing of data and safety.
- *Learning, adaptive and evolving capabilities:* Growing examples of products and systems with learning capabilities. Sometimes systems learn undesired behavior either intentionally or unintentionally (e.g., the Microsoft Tay chatbot that became inappropriate in less than 24 h).
- *Use of predictive and inference analytics:* The ability to do predictive analytics is a new element that may challenge the safety of the user (in case of wrongly predicted or inferred actions). These capabilities can lead to (mis)use for purposes that are unknown to the consumer.
- *Human–product interaction*. There is a growing use of products meant to interact with the users, either physically or cognitively. For instance, robots for children with autism and to support the elderly. These products are meant to interact with the user and it builds trust that goes beyond the mere use of a product.
- *Use of emotions:* Increased use of 'emotional AI.' The ability to read emotions and to make decisions based on that is a growing concern area that we should be (pre)cautious with (Fosch-Villaronga, 2019b). Used normally for marketing purposes and consumer behavior manipulation, the use of these capabilities may go beyond traditional uses and lead to risk scenarios. Facial recognition systems are included in this category.

These new elements, i.e., growing product interconnectivity and machine learning capabilities, increasingly demand a broader cyber-physical approach to ensure product safety. This could be encompassed in an extended concept of safety, which also includes a protection from cyber-security risks. Moreover, the product safety rules should explicitly include protection against risks related to subsequently uploaded software and extended functions acquired by machine learning.

3.1.2. *Medical devices*

Some care robots may be classified as medical devices if they are intended for specific medical purposes, such as diagnosis or treatment. As highlighted recently by the Court, what counts is the real intended purpose and not the mere statement from the producer.[11] The EU's Medical Device Regulation (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) (MDR) contains a detailed definition of medical devices (Art. 2(1)). According to the EU MDR, medical devices must be safe and effective and "shall not compromise the clinical condition or the safety of patients, or the safety and health of users or, where applicable, other persons(…)" (MDR Annex I No. 1). The MDR also requires risk management, and devices must be designed and manufactured in such a way as to remove or reduce as far as possible the risks associated with the possible negative interaction between software and the IT environment within which it operates and interacts (Annex I No. 14.2d)). The most explicit requirement for cybersecurity in the MDR focuses on software, which must be developed "following state of the art taking into account the principles of the development life cycle, risk management, including information security, verification, and validation" (MDR Annex I No.17.2). Medical device manufacturers must also set out minimum requirements concerning hardware, IT networks, and IT security measures, including protection against unauthorised access, necessary to run the software as intended (ibid.).

The MDR directs these requirements to the manufacturer of a medical device. Accordingly, the manufacturer needs to identify and manage cybersecurity risks if a care robot classifies as a medical device. In this sense, other actors involved in the use of a robot, such as hospitals and other care providers, as well as patients, are not directly addressed in the medical device regulation. These actors, however, play a significant role in managing risks related to the actual use of the (robot) device, for example, by installing regular software updates. Other parts of the legal framework (addressed below) focus directly on healthcare providers and those processing personal information. Moreover, the MDR indirectly takes into account these other players in the robot environment, because they are the addressees of instructions for use. These must include appropriate IT security measures (MDR Annex I No. 23.4ab)).

Care robot manufacturers might be unsure of how to comply best with these rules, which are often vague and abstract. Harmonized standards might bring clarity in this respect, although cybersecurity standards for medical robots do not exist yet. Some current standards set out an initial level of requirements regarding cybersecurity. However, they focus more generally on medical device software (European Standard EN 62304 2006) and medical device risk management (European Standard EN 14971 2012) than on care or medical robots. Besides, the ETSI has released a technical specifica-

[11] *See* the judgment of the court for the case C-329/16 Snitem and Philips France: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62016CJ0329&from=EN.

tion focussing on cybersecurity for the internet of things consumers (ETSI TS 103 645:2019), but this is not a 'harmonized standard,' and it does not explicitly focus on either robots or medical devices.

For the context of care robots, cybersecurity requirements for medical devices are significant in two respects. First, these contain essential requirements for care robots that qualify as medical devices. Some robot manufacturers thus need to assess how they can ensure compliance with these requirements, which are defined at a relatively high level of abstraction. The art. 1.3 of the Medical Device Regulation states that 'devices with both a medical and a non-medical intended purpose shall fulfill the requirements applicable to devices cumulatively with an intended medical purpose and those applicable to devices without an intended medical purpose.' This article, at its origin, referred to other devices that had both medical and non-medical purposes. For instance, colored contact lenses had the cosmetics category, although they were medical devices if prescribed. Article 1.3 seems to suggest that those care robots having a medical and a non-medical version, for instance exoskeletons for rehabilitation or for activities of daily living, may have to comply both with the Medical Device Regulation and the Machinery Directive. An example is the case of exoskeletons for activities of daily living or rehabilitation (Fosch-Villaronga and Özcan, 2019). However, the lack of specific regulation brings about uncertainties concerning the application of the current framework to care robot technologies.

Second, these requirements represent the first incorporation of cybersecurity requirements into the EU's regulatory framework for safety. Other legal instruments focusing on safety, which currently lack cybersecurity requirements, could, in theory, be updated with similar rules. Moreover, the EU could even create an entirely new set of cybersecurity rules incorporating new classes of products, such as care robots.

On the other hand, medical device manufacturers (COCIR, 2019) argue that compliance with these and other cybersecurity requirements is challenging, in part due to the potential overlap of different certification schemes with varying geographical or product scope. The European medical device industry (ibid.) has called for the European adoption of a standard form developed in the US, the Manufacturer Disclosure Statement for Medical Device Security (HIMSS/NEMA Standard HN 1-2013 2013). Usually referred to as "MDS2," this form could be used as a means of documenting and communicating medical device security and privacy features in Europe. The MDS2 form is an industry best practice that intends to assist healthcare providers in assessing the vulnerability and risks associated with protecting personal data transmitted or maintained by medical devices and systems. By focusing on personal data, the MSD2 form does not explicitly address the physical manifestation of cyber risks, such as those that can result from the hacking of a robot that physically interacts with humans.

An advantage of the MDS2 form is that it addresses critical issues such as the configuration of security features, cybersecurity product upgrades, malware detection and protection, authentication of people and devices, as well as third party components in a precise manner. The MDS form is essentially a set of questions focusing on aspects such as these, which are significantly more hands-on and relevant than the somewhat abstract wording in the Annex to the EU's MDR.

Cybersecurity is by no means static. New threats can arise, and any actor can update products such as robots in the ecosystem. Adopting a US-developed best practice in the EU may be controversial for political reasons, but the underlying issues are unquestionably global. If an agreement could be reached over concrete problems, a global approach to robot cybersecurity would undoubtedly be advantageous also for the development of a global market for care robots.

3.1.3. *Radio equipment directive*

Care robots may communicate through radio waves, making the rules for radio equipment applicable. The relatively newly revised EU Radio Equipment Directive (2014) contains provisions addressing the protection of personal data and privacy of the users, as well as the protection against fraud (Articles 3(3)(d), (e), and (f)). Although these provisions do not explicitly mention cybersecurity as such, they arguably also require that radio equipment is constructed with a certain level of security. However, these provisions are not yet operational, and their full range is still unclear, pending further implementation. The EU Commission can adopt a delegated act specifying classes of products to which these rules will apply (Article 3(3)), but this has not happened yet. Connected products, including care robots communicating via wireless links, could, in the future, be regulated to protect personal data and against fraud, but so far, these provisions are dormant.

3.2. *Cybersecurity legal framework*

While cybersecurity considerations appear to be an afterthought in the safety legislation, other legislative instruments focus on cybersecurity as a primary concern. As opposed to safety rules, the cybersecurity rules do not provide minimum conditions for putting products on the market. Instead, they focus on ensuring privacy and security in general, independently of the specifics of the product. In the care robot context, these rules do not focus on the robot manufacturer, but on other regulated actors, which we specify in further detail below.

Two legal frameworks partially regulate robot cybersecurity, none of which, however, were designed having robots in mind. The first framework is the Directive on security of network and information systems (also called NIS Directive) that provides measures for boosting the overall cybersecurity in the EU. In the EU's NIS Directive, security is defined as the *ability of networks and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of data*. The second is the EU Cybersecurity Act, i.e., Regulation (EU) 2019/881 which 'establishes an EU-wide cybersecurity certification framework for digital products, services and processes.'

3.2.1. *NIS directive and GDPR*

Care robots can be used in a variety of contexts, such as homes, care facilities, hospitals, and private clinics, which

must ensure an adequate level of security. Some of the involved healthcare providers can have a special legal status as operators of essential services under national laws based on the Network and Information System Security Directive (NIS Directive). According to Art. 14, such operators need to take appropriate and proportionate technical and or-ganizational measures to manage the risks posed to the security of network and information systems that they use in their operations. A Network and Information System can, according to the NIS Directive, include any device or group of interconnected or related devices, which also can encompass physical components such as robots. The underlying interest protected in this context is the essential service of providing healthcare to society. Besides, healthcare providers also process personal data and are, therefore, subject to the provisions of the General Data Protection Regulation (GDPR). They are, according to Arts. 25 and 32 of the GDPR, obliged to implement appropriate measures to ensure a level of security appropriate to relevant risks.

In practice, healthcare providers using care robots can only comply with these obligations if the deployed robots ensure both a basic level of protection and can be maintained and secured to manage risk adequately. In a robot market, consumers might expect robots to include some level of cybersecurity. However, differentiating between higher and lower security of robots is arguably a challenging task, even for a professional robot purchaser. Incomplete and unevenly distributed information about security has long been acknowledged as a challenge in the economic literature on cybersecurity (Asghari et al., 2016, 265).

3.2.2. *EU cybersecurity act*

The deployment and use of care robots require public trust that the robots provide a certain level of cybersecurity. The EU-wide cybersecurity certification schemes could potentially contribute to ensuring such trust in the future. The EU Cybersecurity Act establishes a legal mechanism for voluntary cybersecurity certifications valid in the EU (European Cybersecurity Act 2021). The idea of such certifications in itself is not new. The Act mentions automated cars and electronic medical devices (recital 65) as some examples of sectors in which certification is already widely used or is likely to be used soon. At the same time, cybersecurity certification of ICT products is currently only used to a limited extent, and there do not seem to exist holistic approaches to horizontal cybersecurity issues, for instance, in connection with the Internet of things (recital 67).

The European certification schemes set up by the Act contain a set of rules, technical requirements, standards, and procedures that can be used for the evaluation of the security properties of a specified product. The certificate attests that the product complies with specified requirements. In this sense, the certificate is similar to the CE mark, which indicates conformity with health, safety, and environmental protection standards for products.

A cybersecurity certificate may specify:

- the covered category of products/services;
- the technical standards or specifications or other cybersecurity specifications;
- the type of evaluation, e.g., self-assessment or third-party evaluation; and
- the intended level of assurance.

The Act envisages three assurance levels: basic, substantial, and high (Cybersecurity Act, recitals 88–90). These differ in the level of detail of the technical evaluation. For the basic assurance level, the review focuses only on the technical documentation of the product (recital 88), and it is also possible to self-assess the product or service. For a substantial level, it requires verification of the technology's security functionalities (recital 89), while for the high level, the assurance moreover demands that such security functionalities are tested against elaborate cyberattacks.

So far, it is unclear what kinds of products would be in scope for certification. Existing certifications, such as the ones issued by the German Federal Office of Information Security, have focused, for example, on smart cards. Thus, robots could incorporate security-certified technology. If it was possible to define relevant certification schemes for robots or their components, these could potentially be certified under the EU Cybersecurity Act. The use of certification schemes will be voluntary unless future EU legislation prescribes an EU certificate as a mandatory requirement to satisfy a specific cybersecurity need (Art. 56(2)).

4. Discussion

Some could argue that there is no need to regulate robot cybersecurity because the market will solve this. Indeed, to a certain extent, ensuring robot cybersecurity is in the self-interest of robot developers, manufacturers, and buyers. However, given the competitive pressures from the industry, manufacturers may have incentives for prioritizing a quick market entry and only endeavor to secure their products at a later stage. Building a robot is technically very challenging in many ways, so it would come as no surprise if manufacturers primarily focus on creating robots that can perform a variety of tasks, rather than securing robots against all cyberattacks. Increasing cybersecurity is costly for manufacturers, and they may not be the ones directly affected by any cyberattacks. However, investing in cybersecurity from the design of the technology could promote a safer technology that could prove beneficial for both users and manufacturers in the long run.

According to economic literature (Asghari et al., 2016), introducing measures to align the incentives of actors may improve cybersecurity, so that deviations between private and social costs and benefits are reduced. In principle, the EU laws, as mentioned earlier, should contribute to increasing care robot manufacturers' benefits of increasing cybersecurity in two ways. First, manufacturers are subject to safety regulation, which increasingly includes requirements for cybersecurity. Second, robot purchasers are incentivized to invest in products that help them to ensure compliance with the GDPR, potentially even the NIS Directive, and avoid liability risks. It is clear that the two legal frameworks for, respectively, cybersecurity and safety provide some incentives for ensuring cy-

bersecurity. However, the two frameworks could be better integrated, as discussed below.

Moreover, at a practical level it is not clear whether robot purchasers can distinguish robots with a high level of cybersecurity from those with suboptimal cybersecurity. The introduction of adequate European cybersecurity certificates could potentially alleviate this information asymmetry, by giving robot purchasers some level of assurance about robot cybersecurity.

4.1. *Creating more explicit links between cybersecurity and safety regulation*

The cybersecurity of robots and other connected products is regulated in a fragmented legal framework in need of updating. Basic safety rules focus on one set of actors (including manufacturers), while other rules, such as the GDPR, focus on a different set of actors (including various roles potentially held by robot users). The links between these frameworks are weak, at best.

If a robot's cybersecurity problem is sufficiently grave that it might harm users' safety, then this needs to be addressed by robot manufacturers, who must ensure that the robot is safe. The question is, however, how specific and detailed such cybersecurity assessments are in practice. If the robot is classified as a medical device, the MDR provides some requirements focusing on cybersecurity, which is a good starting point. Alternatively, the general product safety framework applies, where specific cybersecurity requirements are not explicitly stated. In general, the safety concept is sufficiently broad to encompass protection against cybersecurity issues with safety consequences. However, in the absence of clear and specific requirements, it is an open question of whether cybersecurity is sufficiently in focus when manufacturers assess safety risks.

Moreover, safety is not the only concern. Insufficiently secured robots could also affect the users' privacy, or other values, for example, when a robot is used to commit fraud. These would likely not count as safety issues, so they are arguably excluded from the safety framework if safety is interpreted narrowly. Consequently, it is at best unclear whether there is sufficient protection against the marketing of robots that could be used for privacy-invasive or fraudulent purposes. However, this is likely to be remedied in the context of the above-mentioned on-going policymaking regarding the Radio Equipment Directive.

In addition to this safety-related legal framework, the EU's cybersecurity framework also contributes to robot cybersecurity. The GDPR's cybersecurity provisions apply to controllers and processors of personal data, including where such processing is carried out through a robot. Yet the GDPR is concerned with data privacy, while not addressing other values, such as bodily integrity.

Deployers of robot technology might also be liable for damages caused by a robot they use, when a robot causes other harms. However, as highlighted in the recent EU Commission's Whitepaper on Artificial Intelligence (2020a), 'there is some uncertainty about how and to what extent the Product Liability Directive applies in the case [… of] weaknesses in the cybersecurity of the product.' Moreover, due to the complexity of the technology and inherent information asymmetries, it is not easy for robot deployers and users, such as hospital providers or individual robot users, to assess cybersecurity risks.

In summary, the current dual regulatory framework shows the challenges of regulating cyber-physical systems' security. The safety framework does not yet incorporate many explicit requirements for cybersecurity, except for the case of medical devices. On the other hand, the legal framework for cybersecurity focuses on securing selected aspects, such as systems processing personal data and critical sectors, including the health sector.

There exist various options for strengthening the link between cybersecurity and safety (*see* Fig. 2). First, a *horizontal approach* could deal with the issue of cyber-physical security in a single piece of legislation that addresses all connected devices (or at least those for which cybersecurity threats would put users at high risks). On the other hand it is not clear whether such a comprehensive change is needed. A second, *vertical approach* could integrate cybersecurity requirements more explicitly and comprehensively in existing frameworks, including the RED or the Toy Directive, following and expanding on the example of the MDR. This approach would focus on the updating of existing regulations, which is already partly on the way, for example in the revision of the General Product Safety

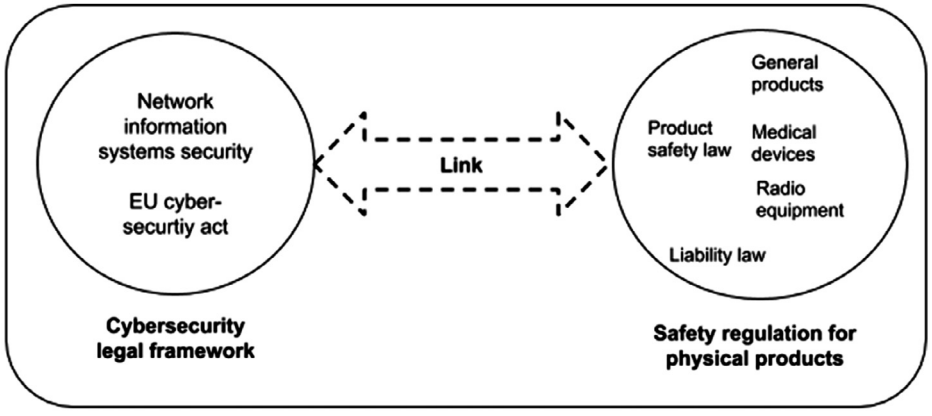

Fig. 2 – Strengthening the link between cybersecurity and product safety regulation in Europe.

Directive.[12] This approach could go in the direction of changing the legal text (i.e., drafting a new definition of safety for products in the Art. 2 b) of GPSD), but it may also be useful to facilitate a flexible interpretation of existing rules (i.e., extending the safety notion to explicitly include cybersecurity aspects).

4.2. *Mandatory cybersecurity certifications and labels*

Under the Cybersecurity Act, certifications are voluntary, unless future EU legislation prescribes an EU certificate as a mandatory requirement to satisfy a specific cybersecurity need (Art. 56(2)). Voluntary certificates could, in theory, add value to the market, because they can provide information about certain security aspects of products and services. On the other hand, most consumers may arguably not be able to understand neither the overall significance of a cybersecurity certificate nor the utility and limitations of the underlying criteria.

European consumer organizations have already called for a mandatory cybersecurity certification for "high-risk connected products," which arguably also includes care robots (Giovanni and Silva, 2018). Similarly, the European Commission has declared that it "will assess whether mandatory certification is required for certain categories of products and services."[13] In the view of the Commission, companies in the EU "will benefit from having to certify their products, processes, and services only once and see their certificates recognized across the Union.'[14]

On the other hand, the European medical device industry (COCIR, 2019) argues that there is a risk that "a patchwork of regulatory requirements may appear," as Member States can introduce their requirements for cybersecurity certification, in addition to EU requirements. In the view of the industry (ibid.), there is no need for a specific mandatory certification scheme for medical devices, "as the MDR introduces security requirements that will become part of the certification for receiving the CE mark." This statement highlights the challenges of integrating the two regulatory frameworks for physical safety and cybersecurity. Indeed, based on the rationale of the *lex specialis* principle, the more specific framework for medical devices might be used as an argument against mandatory cybersecurity certificates for medical devices. Nevertheless, the requirements in the MDR are so general and abstract that there is a need for a more detailed framework for assessing cybersecurity requirements. Such a framework could be created either under the MDR or under the Cybersecurity Act (European Cybersecurity Act 2021).

Moreover, not all care robots necessarily qualify as medical devices. In the view of the medical device industry, other connected technologies and processes in the healthcare setting (i.e., not medical devices), "need to comply with the basic security requirements as set out by self-assessment schemes to be developed under the Cybersecurity Act" (COCIR, 2019).

Given the current absence of cybersecurity schemes, it is too early to assess whether mandatory European cybersecurity certifications are a viable path for achieving an adequate level of cybersecurity for robots, and care robots more specifically. It is going to be interesting to see how cybersecurity certificates and medical device requirements interplay since the two frameworks (the Cybersecurity Act and the MDR) open the possibility for diverging requirements for different classes of products, depending on whether they classify as medical devices or not. On the other hand, it may be the case that cybersecurity certifications defined under the act can be relevant for certain types of robots or components, irrespective of their classification as medical devices.

While voluntary cybersecurity certificates may be relevant for institutional purchasers with specialized knowledge, consumers might be better off with something like the CE mark. First, CE marks are mandatory for certain classes of products (but not generally for all products) and indicate compliance with health, safety, and environmental protection standards for products. CE marks are not certificates, and they have arguably a broader remit than cybersecurity certificates, which certify compliance with particular certification schemes. Although not all consumers understand the significance of CE marks, they are nevertheless a relatively well-known signifier of conformity with specific minimum requirements. On the other hand, the regulatory frameworks that currently require CE-marking products do not cover all types of products, do not necessarily integrate explicit cybersecurity requirements, and thus consumers cannot know whether products are cybersecure.

How can the frameworks for product safety and cybersecurity be integrated? One possibility would be to extend the existing CE-requirements with relevant new requirements focusing on cybersecurity. The first step in this direction is taken in the MDR, but many technical details still need to be defined for medical devices. Further evolution in other product classes requires both a reform of the current safety framework, as well as the development of new harmonized standards to be included in the CE framework.

One of the risks of certifications and labels is that they could lead to users becoming complacent. In other words, certifications would promote users' trust in the system to maintain its security 'on its own.' A further risk is that no certification or mark can guarantee against a brand new kind of attack; all it can really indicate is that the company followed the then best practice at the time of the analysis. Therefore, in the future it is necessary to create dynamic labels that can be updated on-line, based on new developments. Moreover, cybersecurity vulnerabilities arising from new attacks and the continuous learning processes of some of these devices still leave open questions.

5. Conclusions

Exploiting security vulnerabilities of care robots could entail patient harm (Bonaci et al., 2015; Lera et al., 2017; FDA, 2019).

[12] *See* https://ec.europa.eu/transparency/regexpert/index.cfm?do=news.open_doc&id=35114.

[13] *See* https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity.

[14] *See* https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity.

In such sensitive domains of applications as healthcare, this is particularly problematic. Although there is no single legal framework for the cybersecurity of robots, several legal instruments concerning different domains of applications, including GDPR, machinery directive, or medical device regulation, establish requirements relevant to care robots.

The current regulatory framework is dual, as it focuses on safety on the one hand and on cybersecurity on the other hand. In this article, we argued the need of creating more explicit links between cybersecurity and safety regulation. We proposed different options for strengthening such a link between cybersecurity and safety: a *horizontal approach* to dealing with cyber-physical security in a single piece of legislation covering all connected devices; and a *vertical approach* to integrating cybersecurity requirements more explicitly and comprehensively in existing frameworks, including the RED or the Toy Directive, following and expanding on the example of the MDR. This approach goes in line with existing revision efforts the EU Institutions are taking, the General Product Safety Directive revision. This approach could change the legal text or facilitate a flexible interpretation of existing rules (i.e., include cybersecurity aspects explicitly). We also proposed to adopt cybersecurity requirements relevant for CE marking as a way to do justice to the greater implications that cybersecurity has for safety. Overall, the safety framework needs to be updated in light of greater interconnectivity of products, including robots, which raise cybersecurity concerns.

Declaration of Competing Interest

Dr. Eduard Fosch-Villaronga and Prof. Tobias Mahler declare not to have any conflict of interest.

Acknowledgment

Part of this project was funded by the LEaDing Fellows Marie Curie COFUND fellowship, a project that has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie Grant Agreement No. 707404. This research was also financed by the project "Vulnerability in the Robot Society" (VIROS, grant number 144789) and the project "Security in Internet Governance and Networks: Analysing the Law (SIGNAL, grant number 247947), both financed by the Research Council of Norway. The authors wish to thank Lee Bygrave, Peter Davis, Luca Tosoni, Ida Christiane Hunsbedt, Carlos J. Calleja and Gino D'Paola Puche from the University of Oslo, as well as two anonymous reviewers for useful comments on an earlier version of this paper. The usual disclaimer applies nevertheless.

REFERENCES

Alemzadeh H, Raman J, Leveson N, Kalbarczyk Z, Iyer RK. Adverse events in robotic surgery: a retrospective study of 14 years of FDA data. PLoS One 2016;11(4).

Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., & Mané, D. (2016). Concrete problems in AI safety. arXiv preprint arXiv:1606.06565.

Asghari H, van Eeten M, Bauer JM. Economics of cybersecurity. Handbook on the economics of the Internet. Edward Elgar Publishing; 2016.

Ayala L. Cybersecurity for hospitals and healthcare facilities: a guide to detection and prevention. Apress; 2016.

Bonaci, T., Herron, J., Yusuf, T., Yan, J., Kohno, T., & Chizeck, H.J. (2015). To make a robot secure: an experimental analysis of cyber security threats against teleoperated surgical robots. arXiv preprint arXiv:1504.04339 .

Cerrudo, C., & Apa, L. (2017). Hacking robots before SkyNet. *IOActive Website*. Retrieved from https://ioactive.com/pdfs/Hacking-Robots-Before-Skynet.pdf.

Clark GW, Doran MV, Andel TR. Cybersecurity issues in robotics. Proceedings of the 2017 IEEE conference on cognitive and computational aspects of situation management (CogSIMA); 2017. p. 1–5.

COCIR, European coordination committee of the radiological, electromedical and healthcare IT industry (2019). Advancing cybersecurity of health and digital technologies. Retrieved from https://www.cocir.org/uploads/media/19036_COC_Cybersecurity_web.pdf.

Cresswell K, Cunningham-Burley S, Sheikh A. Health care robotics: qualitative exploration of key challenges and future directions. J Med Internet Res 2018;20(7):e10410.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194. 2016

Directive (EU) 2014/53 of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment, OJ L 153/62.2014

Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety.2001

Dolic Z, Castro R, Moarcas A. Robots in healthcare: a solution or a problem?, Study for the committee on environment, public health, and food safety. Luxembourg: Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament; 2019 Retrieved from https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/638391/IPOL_IDA(2019)638391_EN.pdf .

European Commission (2016). Guide to the implementation of directives based on the new approach and global approach, retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016XC0726(02)

European Commission (2020a) Whitepaper on artificial intelligence – a European approach to excellence and trust. Retrieved from https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

European Commission (2020b) Impact assessment on increased protection of internet-connected radio equipment and wearable radio equipment. Retrieved from https://ec.europa.eu/docsroom/documents/40763/attachments/2/translations/en/renditions/native (accessed 26 September 2020).

European Commission (2020c) Report on the safety and liability implications of artificial intelligence, the internet of things and robotics, retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0064&from=en (accessed 11 November 2020).

European Cybersecurity Act. Retrieved from https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.2021

European Foresight Monitoring Network, EFMN (2008) Roadmap robotics for healthcare. Foresight brief no. 157. Retrieved from, http://www.foresight-platform.eu/wp-content/uploads/2011/02/EFMN-Brief-No.-157_Robotics-for-Healthcare.pdf.

European Standard EN 62304:2006 A1:2015. Medical device software – software life-cycle processes.
European Standard EN 14971:2012. Medical devices – application of risk management to medical devices.
European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). Retrieved from http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.pdf.2017
European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics (2018/2088(INI)). Retrieved from http://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_EN.pdf.2018
Expert Group on Liability and New Technologies. Liability for artificial intelligence and other emerging digital technologies. European Commission; 2019 Retrieved from https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608 .
Food and Drug Administration, FDA (2019) Cybersecurity. Retrieved from: https://www.fda.gov/medical-devices/digital-health/cybersecurity.
Fosch-Villaronga E. (2016) ISO 13482:2014 and its confusing categories. Building a bridge between law and robotics. In: Wenger P., Chevallereau C., Pisla D., Bleuler H., Rodić A. (Eds.) *New trends in medical and service robots. Mechanisms and machine science*, Springer, Cham., 39, 31–44.
Fosch-Villaronga E. Robots, healthcare, and the law. Regulating automation in personal care. Routledge; 2019a.
Fosch-Villaronga E, Ayanoğlu H, Duarte E. I Love You," Said the Robot: boundaries of the use of emotions in human-robot interactions. Emotional design in human-robot interaction. Cham: Springer; 2019b. p. 93–110.
Fosch-Villaronga E, Felzmann H, Ramos-Montero M, Mahler T. Cloud services for robotic nurses? Assessing legal and ethical issues in the use of cloud services for healthcare robots. Proceedings of the 2018 IEEE/RSJ international conference on intelligent robots and systems (IROS); 2018. p. 290–6.
Fosch-Villaronga E, Golia Jr A. Robots, standards and the law: rivalries between private standards and public policymaking for robot governance. Comput Law Secur Rev 2019a;35(2):129–44.
Fosch-Villaronga E, Golia Jr A. The intricate relationships between private standards and public policymaking in the case of personal care robots Who cares more. In: Barattini P, Vicentini F, Virk GS, Haidegger T, editors. Human-robot interaction: safety, standardization, and benchmarking (2019). CRC Press; 2019b.
Fosch-Villaronga E, Millard C. Cloud robotics law and regulation: challenges in the Governance of complex and dynamic cyber-physical ecosystems. Rob Auton Syst 2019;119:77–91.
Fosch-Villaronga E, Özcan B. The progressive intertwinement between design, human needs and the regulation of care technology: the case of lower-limb exoskeletons. Int J Soc Robot 2019:1–14.
Fosch-Villaronga, E. & Drukarch, H. G., (2021) AI for Healthcare Robots. AI for Everything Series. CRC Press (forthcoming).
Giovanni, C., Silva, F. (2018). Cybersecurity for connected products. ANEC/BEUC Position Paper. Retrieved from https://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf.
HIMSS/NEMA Standard HN 1-2013. Manufacturer disclosure statement for medical device security. Retrieved from https://www.himss.org/resourcelibrary/MDS2.2013
Holder C, Khurana V, Harrison F, Jacobs L. Robotics and law: key legal and regulatory implications of the robotics age (Part I of II). Comput Law Secur Rev 2016;32(3):383–402.
Holloway, S. (2015). Stuxnet Worm Attack on Iranian Nuclear Facilities. Online article. Retrieved from: http://large.stanford.edu/courses/2015/ph241/holloway1/, last accessed March 27, 2020.
ISO 8373:2012 Robots and robotic devices – vocabulary.
Johnson SD, Blythe JM, Manning M, Wong GTW. The impact of IoT security labelling on consumer product choice and willingness to pay. PLoS One 2020;15(1). doi:10.1371/journal.pone.0227800.
Leenes R, Palmerini E, Koops BJ, Bertolini A, Salvini P, Lucivero F. Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues. Law Innov Technol 2017;9(1):1–44.
Lera FJR, Llamas CF, Guerrero ÁM, Olivera VM. Cybersecurity of robotics and autonomous systems: privacy and safety. In: Dekoulis G, editor. Robotics: legal, ethical and socioeconomic impacts (2017).. IntechOpen; 2017 https://cdn.intechopen.com/pdfs/56025.pdf.
Medical Device Coordination Group, MDCG (2019) Guidance on cybersecurity for medical devices. Retrieved from https://ec.europa.eu/docsroom/documents/38941/attachments/1/translations/en/renditions/native (last accessed 26 September 2020).
Morante S, Victores JG, Balaguer C. Cryptobotics: Why robots need cyber safety. Front Robot AI 2015;2:23.
Michels JD, Walden I. How Safe is Safe Enough? Improving Cybersecurity in Europe's Critical Infrastructure Under the NIS Directive. Improving Cybersecurity in Europe's Critical Infrastructure Under the NIS Directive (December 7, 2018). Queen Mary School of Law Legal Studies Research Paper, 2018 (291).
Quarta D, Pogliani M, Polino M, Maggi F, Zanchettin AM, Zanero S. An experimental security analysis of an industrial robot controller. Proceedings of the 2017 IEEE symposium on security and privacy (SP); 2017. p. 268–86.
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
Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). 2019
Simshaw D, Terry N, Hauser K, Cummings ML. Regulating healthcare robots: maximizing opportunities while minimizing risks. Rich JL Tech 2015;22(1) https://heinonline.org/HOL/Page?handle=hein.journals/jolt22&div=6&g_sent=1&casa_token=&collection=journals.
Wedmid A, Llukani E, Lee DI. Future perspectives in robotic surgery. BJU Int 2011;108(6b):1028–36 https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1464-410X.2011.10458.x.
World Commission on the Ethics of Scientific Knowledge and Technology (COMEST). Report of COMEST on Robotics Ethics. SHS/YES/COMEST-10/17/2 REV. Retrieved from https://unescoblob.blob.core.windows.net/pdf/UploadCKEditor/REPORT%20OF%20COMEST%20ON%20ROBOTICS%20ETHICS%2014.09.17.pdf. 2017, last accessed 07 Jan 2021.
Yang GZ, Cambias J, Cleary K, Daimler E, Drake J, Dupont PE, et al. Medical robotics—regulatory, ethical, and legal considerations for increasing levels of autonomy. Sci Robot 2017;2(4):8638 http://robotics.tch.harvard.edu/publications/pdfs/yang2017medical.pdf.