Research article
DOI: https://doi.org/10.21202/jdtl.2023.2

Regulating Smart Robots and Artificial Intelligence in the European Union

Chiara Gallese Nobile

Eindhoven University of Technology
Eindhoven, Kingdom of the Netherlands;
University of Trieste
Trieste, Italian Republic

Keywords

Artificial intelligence,
cybersecurity,
digital technologies,
European Union,
law,
legislation,
machine learning,
regulation,
robot,
robotics

Abstract

Objective: In recent years, the need for regulation of robots and Artificial Intelligence has become apparent in Europe. European Union needs a standardized regulation that will ensure a high level of security in robotics systems to prevent potential breaches. Therefore a new regulation should make clear that it is the responsibility of producers to identify the blind spots in these systems, exposing their flaws, or, when a vulnerability is discovered in a later stage, to update the system even if that model is not on the market anymore. This article aims at suggesting some possible revisions of the existing legal provisions in the EU.

Methods: The author employed the Kestemont legal methodology, analyzing legal text, comparing them, and connecting them with technical elements regarding smart robots, resulting in the highlighting of the critical provisions to be updated.

Results: This article suggests some revisions to the existing regulatory proposals: according to the author, although the AI Act and the Cyber-resilience Act represent a first step towards this direction, their general principles are not sufficiently detailed to guide programmers on how to implement them in practice, and policymakers should carefully assess in what cases lifelong learning models should be allowed to the market. The author suggests that the current proposal regarding mandatory updates should be expanded, as five years are a short time frame that would not cover the risks associated with long-lasting products, such as vehicles.

Scientific novelty: The author has examined the existing regulatory framework regarding AI systems and devices with digital elements, highlighted the risks of the current legal framework, and suggested possible amendments to the existing regulatory proposals.

Practical significance: The article can be employed to update the existing proposals for the AI Act and the Cyber-resilience Act.

For citation

Gallese Nobile, C. (2023). Regulating Smart Robots and Artificial Intelligence in the European Union. *Journal of Digital Technologies and Law*, *1*(1), 33–61. https://doi.org/10.21202/jdtl.2023.2

Contents

Introduction

Despite the remarkable successes of the NIS Directive and the effort to update the discipline with the NIS II, Cyber-resilience Act, and AI Act proposals, the theme of cybersecurity in the digital age is still crucial for the European market. The regulatory instruments helped several Member States adapt their institutional, regulatory, and attitude toward cybersecurity, but the availability of new technologies such as AI systems and unprecedented circumstances, such as the COVID-19 pandemic, have escalated society's digital transition, increasing the threat landscape and creating new issues that need to be addressed at both national and international level. Cyberattacks are becoming more frequent, and they're getting more advanced as they come from both inside and outside the EU, often creating significant

risks for rights and freedoms of citizens[1]. As more hardware and software goods are the targets of successful cyberattacks, it is predicted that, by 2021, the yearly worldwide cost of cybercrime would reach 5.5 trillion of euros.

The explanatory memorandum attached to the Cyber-resilience Act evidenced how inadequate understanding and information availability for users prevents them from selecting products with adequate cybersecurity properties and causes an unsafe use[2]. Such items are plagued by two serious challenges that add costs for users and society: (1) a lack of adequate of information security, evidenced by pervasive security breaches and the inadequate and inconstant delivery of security updates to handle them; and (2) a low degree of knowledge and information accessibility by users[3]. A cybersecurity attack affecting a single product can have an impact on the entire organization or supply chain, frequently spreading beyond internal market borders in a very short time[4].

A reform of the cybersecurity legal framework received the support from enterprises and competent authorities. They indicated, during numerous consultations, that the NIS Directive should be modified to include more subsectors, integrate or optimize additional security measures, and simplify reporting requirements[5]. This shows how the cybersecurity problem is perceived as an important topic to be addressed at the institutional level.

This article provides some insights on the problems arising from connected smart robots within the European legal system, proposing some suggestions for an update of the discipline. It first provides some insights regarding the definition of Artificial Intelligence (AI) and Smart Robot and describes the regulatory framework on the topic. It then draws some considerations regarding machine learning and black boxes, highlighting some issues that need to be addressed at the EU level. Finally, it briefly analyzes some shortcomings of the proposal for a Cyber-resilience Act.

1 Commission Staff Working document Delivering on the UN's Sustainable Development Goals – A comprehensive approach: https://sdgtoolkit.org/wp-content/uploads/2021/02/EU-staff_working_document-delivering_on_uns_sustainable_development_goals_en.pdf

2 European Commission. (2022). https://ireland.representation.ec.europa.eu/news-and-events/news/new-eu-cybersecurity-rules-ensure-more-secure-hardware-and-software-products-2022-09-15_en

3 *Ibid.*

4 *Ibid.*

5 Commission Staff Working document Delivering on the UN's Sustainable Development Goals – A comprehensive approach. https://sdgtoolkit.org/wp-content/uploads/2021/02/EU-staff_working_document-delivering_on_uns_sustainable_development_goals_en.pdf

1. Artificial Intelligence and Robots: definitions

In the last decade, the use of AI-driven systems, including robots, especially the ones using machine learning, has reached a remarkable extent and it will increase even more in the future (Wang & Siau, 2019). Some examples of their actual application include drones (De Swarte et al., 2019), self-driving cars (Rao & Frtunikj, 2018), medical devices (O'Sullivanet al., 2019) and diagnosis (Nobile et al., 2019), home assistants (Yuniarthe, 2017), robots for elderly care (Simoens et al., 2016) and co-human work (Demir et al., 2019), translators (Bi, 2020), image recognition (Rundo et al., 2019), insurances (Lamberton et al. 2017), predictions (e.g. in judicial decisions (Sourdin, 2018) or finance), emergency communication (Raza et al., 2020), HR (Yano, 2017), traffic control (Aladin et al., 2019), e-mail management (including spam filters (Das et al., 2015)), construction (Chakkravarthy, 2019), logistic (Pandian, 2019), education (Roll & Wylie, 2016), and many other fields. Following this fast development, the aim for legal certainty related to new technologies has been on the EU agenda for several years.

The level that has been achieved in the AI field is very far from the one theorized by Turing ("strong AI"). The present AI is called "Artificial Narrow Intelligence (ANI)" (Kaplan & Haenlein, 2019) or "weak AI" (Lu et al., 2018) and it consists of systems dedicated to specific tasks, based on models and algorithms designed and calibrated by human beings on the basis of data and parameters chosen at the discretion of the model-maker. This means that it is able to perform specific tasks, sometimes even better than human beings, but it cannot transfer those skills into other fields of knowledge. The term "¨Intelligence" is, therefore, quite misleading.

It is primarily important to define the relevant law terminology, as legal definitions often do not coincide with those of computer scientists (Smith, 2016), who, at the same time, are not always unanimous (Bekey, 2012).

The proposal for an European regulation on AI (the so-called AI Act)[6]has listed the techniques that are considered as AI at EU level; in that document, the proposed definition of "Artificial Intelligence System" is very broad and includes techniques that have been known for decades: "[...] software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with"; in fact, the list in Annex I considers a wide range of different techniques: "(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and

6 The proposal is accessible at the following address: https://ec.europa.eu/newsroom/dae/items/709090

expert systems; (c) Statistical approaches, Bayesian estimation, search and optimization methods". The goal of this definition is to include many different models that could have an effect on citizens, even those that are not always defined as AI. In this way, it would be difficult to elude the application of the regulation just changing the definition of a model in a way that does not relate it to AI. However, this definition has raised some criticisms as it is deemed to be too broad[7].

Finding a proper definition of the term "robot" is difficult. According to the High-Expert Group, "Robotics can be defined as "AI in action in the physical world" (also called embodied AI). A robot is a physical machine that has to cope with the dynamics, the uncertainties, and the complexity of the physical world. Perception, reasoning, action, learning, as well as interaction capabilities with other systems are usually integrated in the control architecture of the robotic system. In addition to AI, other disciplines play a role in robot design and operation, such as mechanical engineering and control theory. Examples of robots include robotic manipulators, autonomous vehicles (e.g. cars, drones, flying taxis), humanoid robots, robotic vacuum cleaners, etc.".

According to the "European civil law rules in robotics" study (Nevejans, 2016), on the other hand, since there is no consensus within the scientific community regarding the definition of robots, there are still some terminological issues regarding the terms "smart robot" and "autonomous robot" (Haselager, 2005). Some authors have referred to the definition of Richards and Smart (Richards & Smart, 2016), according to whom a robot is "a constructed system that displays both physical and mental agency, but is not alive in the biological sense", but the discussion about agency is too broad for a thorough treatment here, and it will be explored in a different article.

In order to be considered as a "smart robot" from a legal point of view – according to the European Parliament resolution of 16 February 2017 with recommendations to the commission on civil law rules on robotics (European Parliament, 2017) – an entity should meet the following conditions:

– the acquisition of autonomy through sensors and/or by exchanging data with its environment (inter-connectivity) and the trading and analysing of those data;

– self-learning from experience and by interaction (optional criterion);

– at least a minor physical support;

– the adaptation of its behaviour and actions to the environment;

– the absence of life in the biological sense.

[7] For example, in the Draft Opinion of the Committee on Industry, Research and Energy for the Committee on the Internal Market and Consumer Protection and the Committee on Civil Liberties, Justice and Home Affairs, available at: https://www.europarl.europa.eu/doceo/document/ITRE-PA-719801_EN.pdf , and in the Draft Opinion of the Committee on Legal Affairs for the Committee on the Internal Market and Consumer Protection and the Committee on Civil Liberties, Justice and Home Affairs.

Definitions are very important when amending existing regulations or issuing new laws, as many cases could be left out of the scope of the provisions if they do not fall within the legal definition. Nevertheless, it has been noted that any attempt at providing an encompassing definition is a fruitless exercise since robotic applications are extremely diverse (Bertolini, 2013). In this paper, we will use the term "device" to generally refer to AI-driven instruments and robots, regardless of their kind, and "software" or "model" to refer to the AI systems, including those installed in such devices.

It is our opinion that, from a legal point of view, there is little difference between a machine which we can define"robot" and an AI-driven device which cannot be strictly defined as a "robot" but is still "smart" and can have an impact on the outside environment. Sometimes the difference between the twoconcepts is quite labile. For example, are a smart dishwasher or an autonomous vacuum robots? Is it an autonomous car? Is it a home assistant or a cellphone that can control a house's doors, lights, dampers, garage tilting, and such? And what about a 4D printer? If they are not, what would be the legal difference?

According to the definition given by the above-mentioned resolution, even a duck-shaped toy (absence of life and physical support) that moves around the room and changes direction when the wheels are blocked by an obstacle (adaptation to environment), which has a timer to wake up itself, and performs a different song whenever the light changes (acquisition of autonomy through sensors), it is considered a smart robot, even if it could be entirely built through electrical circuits and mechanical parts without any piece of software or AI model.

The definition, therefore, looks rather vague and not sufficient to fully describe a smart robot, and it embraces machines that have no AI at all.

Some have argued that the key aspect of a robot relies on its ability to execute a software to carry out specific tasks (Leenes et al., 2017), but, in our opinion, this is not correct (it would be also the definition of a computer!); in fact, nor the performing of autonomous tasks (Santosuosso et al., 2012) nor the presence of software can be used to distinguish a robot from other machines. For example, one thing to keep in mind is that robots could be built with physical components like memristive devices, which may be used similarly to biological synapses in neuromorphic hardware (Ames et al., 2012), without any software inside it.

Software can be loaded in a robot but can exist outside it too, as in the case of virtual robots, which are subject to the regulations regarding software. Moreover, the physical components of a robot can be independent with respect to a specific software, that can be replaced and sold separately. The code running in a robot can be implemented as a monolithic software, but it is often architecturally composed of multiple interacting sub-modules, where each component performs a separate and specific task.

An important distinction within the AI domain should be made between the concepts of software, neuromorphic devices and circuits, and Field Programmable Gate Array (FPGA).

Different techniques can be combined, as in Heildeberg's Spikey chip[8]. All solutions can be used to build a smart robot, but the legal consequences for producers and programmers may be different.

Neuromorphic devices (Ielmini & Ambrogio, 2019) and circuits (Pan et al., 2020), on the contrary, are physical objects and function only on the specific robot they are built in, designed to perform neural computation but also used to simulate the dynamics of biological neural networks (Papetti et al., 2020). FPGAs (Botros & Abdul-Aziz, 1994) is an intermediate solution between the two: it is an integrated physical circuit that can be configured by a final user or by a programmer.

All these solutions may be used to make a robot and, in the future, possibly, to build a functioning physical artificial brain.

Being programmed is not an essential feature of robots, either: for example, in principle it is possible to create a magnetic modular robot that moves, performs actions autonomously, and communicates with other robots through lights, without its builder knowing what its behaviour will be, similarly to the concept of M-cubes (Romanishin et al., 2013).

We believe that AI-driven software that can be installed in any kind of device should have a homogeneous discipline, regardless of whether it is installed in a machine that currently has the formal status of robot or not, and on the contrary, we believe that non-smart robots, especially if not connected to the internet, such as industrial robots in the assembly line, should be subject to the ordinary discipline regarding defective products and to the other regulations applicable to machines. The line should be drawn taking into consideration the effects on society and on people, not on the presence of a physical body.

The main reason to bring together robots and AI-based software under the same discipline is the fact that, if the two were separated, it would be possible to sell separately both the software and the machine without being subject to the regulations regarding smart robots. Any user could install different software to build a smart robot, programming it to perform any activity. It should be noted that, according to the prevailing opinion, a machine directed by a person through remote control, so that a human must be present to carry out certain tasks or to take control of the device, cannot be considered a robot (Ebers & Navas, 2020; Funkhouser, 2013). Therefore, the physical machine without any software installed on it (or accessible by it, such as in case of a software running on the cloud) cannot be considered a robot as well.

It is worth mentioning that a robot utilized in the industry is considered a machine, therefore it is subject to Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 and to Directive 95/16/EC32.

8 Additional information can be found in the following website: https://www.kip.uni-heidelberg.de/vision/previous-projects/facets/neuromorphic-hardware/single-chip-system/spikey/

The European AI Act proposal, in fact, makes reference to the Machinery Directive to include smart robots into the general regulation of AI, thus bringing together both physical robots and virtual robots.

2. Regulating AI and smart robots in the EU: technical regulations

After the theme of AI has become more and more discussed among computer scientists all over the world, European legal scholars and policy-makers have started to debate about legal aspects of AI and smart robots, focusing mainly on product liability and consumer protection, as well as on technical regulation. The legal doctrine has recognized the urgent need for the implementation of harmonized sectoral technical regulations that could meet the needs of the variety of different robotic technologies (Amidei, 2017).

Many legal opinions regarding incidents caused by a robot or by an AI-driven device, however, have considered the problem from an ex post perspective. Nevertheless, it is important to consider as well how to prevent accidents from occurring, especially with regards to cyber-security. Even if it is not possible to avoid any attack in toto, it is important that the matter is analyzed from a risk prevention perspective (the same rationale leading the Directive on machinery), and the new AI Act proposal is going towards this direction.

The most important innovation of the AI Act proposal is the establishment of four risks categories for AI systems, in order to protect citizens' fundamental rights [9].

[9] The explanatory memorandum attached to the proposal, in fact, notes that "The use of AI with its specific characteristics (e.g. opacity, complexity, dependency on data, autonomous behaviour) can adversely affect a number of fundamental rights enshrined in the EU Charter of Fundamental Rights ('the Charter'). This proposal seeks to ensure a high level of protection for those fundamental rights and aims to address various sources of risks through a clearly defined risk-based approach. With a set of requirements for trustworthy AI and proportionate obligations on all value chain participants, the proposal will enhance and promote the protection of the rights protected by the Charter: the right to human dignity (Article 1), respect for private life and protection of personal data (Articles 7 and 8), non-discrimination (Article 21) and equality between women and men (Article 23). It aims to prevent a chilling effect on the rights to freedom of expression (Article 11) and freedom of assembly (Article 12), to ensure protection of the right to an effective remedy and to a fair trial, the rights of defence and the presumption of innocence (Articles 47 and 48), as well as the general principle of good administration. Furthermore, as applicable in certain domains, the proposal will positively affect the rights of a number of special groups, such as the workers' rights to fair and just working conditions (Article 31), a high level of consumer protection (Article 28), the rights of the child (Article 24) and the integration of persons with disabilities (Article 26). The right to a high level of environmental protection and the improvement of the quality of the environment (Article 37) is also relevant, including in relation to the health and safety of people. The obligations for ex ante testing, risk management and human oversight will also facilitate the respect of other fundamental rights by minimising the risk of erroneous or biased AI-assisted decisions in critical areas such as education and training, employment, important services, law enforcement and the judiciary. In case infringements of fundamental rights still happen, effective redress for affected persons will be made possible by ensuring transparency and traceability of the AI systems coupled with strong ex post controls".

The risk categories are related to the degree (intensity and scope) of risk for the safety or fundamental rights of citizens and are classified in three different groups (four, if we consider the"no risk" category):

– (i) unacceptablerisk,

– (ii) highrisk,

– (iii) low or minimal risk.

Taking inspiration from the product safety legislation, the classification of risks is based on the intended purpose and modalities for which the AI system is used, not only on their specific function [10]. The proposal also draws up a list of prohibited AI systems that fall within the first risk category.

In this framework, smart robots are classified as high risk (in fact, as said, reference is made to the Machinery Directive). Because of this classification, new requirements are drawn, and programmers/producers are forced to implement the following:

Risk management system;

Data governance system;

Transparency measures;

Human oversight measures;

Accuracy, robustness and cybersecurity measures;

Quality management system.

After the AI Act proposal, the European Commission has published a new proposal regarding cybersecurity: the so-called Cyber-resilience Act[11], with the aim of ensuring 1) an improved security of products with digital elements throughout their whole life cycle; 2) an harmonized European cybersecurity framework; 3) an improved transparency of security properties of such products; 4) a better safety of such products for businesses and consumers.

In addition to this new framework, two other relevant proposals were published: the AI Liability Directive and a revision of the Product Liability Directive.

In the following sections we will see how these requirements may be implemented and expanded with new provisions during the review phase of the new regulation.

3. Regulatory solutions to prevent cyber attacks

We should take into consideration that the more the technology advances, the more we discover bugs and flaws in the old and obsolete software (Buchanan, 2016), which are exposed to cyber threats (Ozkan & Bulkan, 2019) and require security updates. Some examples of recent attacks include the first known death from a cyber-attack occurred

[10] Depending on the national legal system, the qualification of high risk may have consequences over liability, such as that under art. 2050 of the Italian Civil Code.

[11] Cyber-resilience Act. https://ireland.representation.ec.europa.eu/news-and-events/news/new-eu-cybersecurity-rules-ensure-more-secure-hardware-and-software-products-2022-09-15_en

in September 2020 because of delayed care after cyber-criminals hacked 30 computers in a hospital in Dusseldorf, Germany, with ransomware[12]; the hacking of smart security cameras in 2019, that lead to a class-action lawsuit in the US[13]; the discovery of St. Jude Medical's implantable cardiac devices' vulnerabilities that could allow a hacker to access a device depleting the battery, or administering incorrect pacing or shocks[14]; the Mirai botnet (Zhang et al., 2020), that has been attacking several IoT devices since 2016. Sometimes, the threats to AI-driven systems are physical: in the literature, there are examples that show how colour patches[15] can interfere with the neural network used by autonomous vehicles (Ranjan et al., 2019), leading to misclassifications or wrong interpretation of signals, and therefore they can cause accidents.

It is clear that fighting cyber-attacks is of utmost importance when fundamental rights are at stake, like in the healthcare sector, which is particularly targeted (Luna et al., 2016), or in the case of autonomous vehicles, military devices, satellites and other devices used for national defence.

Manufacturers and programmers are constantly updating their software and devices until they move to a new product or a new version of an existing product. After some time, they stop to develop security patches and updates for the older devices, as it would be too expensive to keep thousands of products on the market when very few customers would buy them and to develop updates for those products that are no longer on the market.

To make software or operating systems work on their hardware, device manufacturers must write drivers specifically for their devices, as they are often closed-source, hence they can only be updated by said manufacturer. This means that old and obsolete devices, operating systems, and software, at a certain point, remain without protection (e.g., Windows XP, used by nearly 4 percent of machines worldwide even if it is not updated by Microsoft anymore), thus being an easy target for attackers. In some cases, manufacturers are willing to update their devices, but they are not able to do so because there are only a few people left who can understand and properly use an old or exotic programming language (e.g., COBOL, used by banks; ADA, used for military applications, air traffic control, commercial rockets, satellites, railway and high-speed transport; FORTRAN, used for scientific computing), or because the source code is too long and too complicated to change.

---

12 The detailed news is reported here: www.bbc.com/news/technology-54204356 (last accessed 14 November 2020). Ransomware is a type of malware that blocks access to the victim's data or sometimes threatens to disclose them to third parties unless the victim pays a certain amount of money.

13 The complete text can be found here: https://www.courtlistener.com/docket/16630199/1/orange-v-ring-llc (last accessed 15 November 2020).

14 The news has been reported by CNN: https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack (last accessed 15 November 2020).

15 A colour patch is a type of adversarial patch, a machine learning technique that attempts to fool neural networks by providing deceptive inputs, in order to cause a malfunction.

If the current system remains in place, it is likely that producers will not update their smart robots for their whole life because, under the current discipline, producers are no longer held responsible after 3 years from the time in which the user discovered the damage, with a limit of 10 years, while the Cyber-resilience Act only propose a 5-years protection. However, some robots will possibly have a life of more than ten years (such as cars, which become even more valuable after 30 years, see, for instance, the Italian concept of "auto d'epoca"), and will consequently remain without protection after a few years.

The technical regulation of these issues can be reached in three ways: banning obsolete technology that represents a risk for people's fundamental rights; forcing manufacturers to update obsolete software and devices; or a regime that mixes both of those two solutions. Each has benefits and downsides.

Lastly, for the purpose of creating a new regulation on smart robots, different robots characteristics should be taken into account, in order to create specific provisions for each of them. For example, some robots are independently created by an interaction between objects (e.g., a new entity made by modular robots, or, in the future, robots created by other robots), therefore it is difficult for humans to predict how they will be assembled. This type of robots should be put in the high risk category, due to their unpredictable behaviour. Some robots move or have an influence to the environment, potentially posing a risk to harm humans, while others are unable to do so (e.g., traffic lights). Some of them operate without human supervision (such as automatic trading on the stock market), posing a significant risk, while some others are directly guided by humans or by other external forces (such as lights, sounds, chemicals, magnets, electricity, or even animals); some make actions or take "decisions" that have a significant impact on individual rights, some others have a limited impact. Finally, some are connected to the internet or to another network (IoT), potentially being exposed to cyber attacks, some are not. All these elements should be carefully considered by regulators when implementing technical regulations.

The new AI Act proposal does not go that far in regulating smart robots. In fact, the provision about cyber-security is vague: "Article 15 Accuracy, robustness and cybersecurity 1. High-risk AI systems shall be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle. 2. The levels of accuracy and the relevant accuracy metrics of high-risk AI systems shall be declared in the accompanying instructions of use. 3. High-risk AI systems shall be resilient as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems. The robustness of high-risk AI systems may be achieved through technical redundancy solutions, which may include backup or fail-safe plans. High-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way to ensure that possibly biased

outputs due to outputs used as an input for future operations ('feedback loops') are duly addressed with appropriate mitigation measures. 4. High-risk AI systems shall be resilient as regards attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities. The technical solutions aimed at ensuring the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks. The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent and control for attacks trying to manipulate the training dataset ('data poisoning'), inputs designed to cause the model to make a mistake ('adversarial examples'), or model flaws".

In the next section we will focus on machine learning (supervised or unsupervised) and black-boxes, due to their peculiar characteristics.

3.1. Machine Learning and black-boxes

Although a sci-fi-oriented narrative has made the public used to an image of intelligent self-learning robots, only a small part of all robots is programmed to learn by experience. Some of them look smart because they perform difficult tasks and interact with the environment, but they are actually only programmed using simple algorithms.

From a legal perspective, models based on machine learning (especially deep learning and continuous learning) deserve particular attention due to their peculiar characteristics, therefore they will be discussed in a separate subsection.

3.1.1. Security regulations and standards for machine learning models

As it is known, it is not possible to a priori exclude the presence of biases or bugs (Naur & Randell, 1968) that could influence the behavior or the decisions taken by an AI device. In fact, the model is developed by a human being, who is, of course, fallible. This means that a programmer will never be able to ensure that the model behaves exactly as programmed[16], but it also means that, by changing hyper-parameters and selecting the data conveniently (or politically), the same tool can be used to obtain different results.

The data utilized can, in itself, represent a relevant problem: they can be wrong, false, incomplete, or simply too few to be meaningful[17], therefore the result will not be reliable; moreover, even if the data are correct, artificial intelligence can reach conclusions that are

[16] Even running a large number of tests, it is not possible to exclude the presence of bugs. Quoting the renowned computer scientist and Turing prize recipient E.W. Dijkstra (1982), "testing shows the presence, not the absence of bugs" (Dijkstra, 1982).

[17] In fact, to train a Machine Learning model it is often necessary to use thousands of examples.

prejudicial to certain categories[18], based on dynamics deriving from inequalities present in society, which, in the end, can confuse the relationship between cause and effect, as shown in some famous cases (Falletti, 2020).

Against this background, it is crucial to define some essential rules and standards that must be met by the AI model before it is released into the market. In our opinion, an AI should be modelled following these general criteria, some of which are already present in the ALTAI list:

– it should be understandable (the most used terms in literature are transparency, interpretability, explainability, and explicability (Chakraborti et al., 2019; Gilpin et al., 2018; Holzinger et al., 2019), but we believe that the correct term should be "Interpretability"), i. e., the model should be transparent in the ways through which it reaches its decisions, so that it would always be possible to understand the reasoning behind its choices, and the output and the rationale of decisions of the model should always be understandable by humans;

– it should follow privacy by design and by default principles (Hildebrandt, 2019), i. e., the model should meet the GDPR requirements in order to protect user's and third parties' data, and the consent for the use of said data should be well informed[19];

– it should be ethical (Greene et al., 2019), i.e., there should be rules to avoid any discriminatory behaviour that could emerge when the robot is released into society, albeit not yet covered by existing law[20];

– it should be unbiased (Dietterich & Kong, 1995), i.e., the training of the AI should be reviewed by experts to eliminate any possible bias, in order to make it trustworthy and accurate while at the same time complying with applicable laws and regulations[21];

– it should be updated and secure (Barreno et al., 2010), i.e., updates and patches should be implemented and tests should be run on a regular basis, and the mechanical part should be regularly inspected too, providing support throughout the whole life of the robot;

---

18 Legal aspects of machine learning in relation to possible bias and their effects on vulnerable groups will be explored in a separate article, as the topic is too broad to be addressed here.

19 Although this element is already present in the European legislation, EU citizens may still be subject to adverse events when their data is collected by AI systems outside the EU.

20 It must be noted that in this paper we do not exclusively consider the rights that are actually protected by law in each legal system, since the fact that a certain right is not yet recognized by a State does not mean that such right does not exist, or that it should not be introduced in that system. Some problems arising from the use of AI are not derived from bugs or other types of programming mistakes but from political choices or unconscious human biases. For example, a system that is aimed at helping the health care system to perform cervix cancer screening could be programmed to cover costs and send invitations only to individuals over 40 years old registered as females.

21 It is important to note that we use the word "bias" from a legal studies point of view, which is different from that of computer scientists; in fact, if we consider only the programmer's perspective, it can be argued that a truly unbiased model could never exist. In this paper, we only consider biases that, from a legal and ethical point of view, could lead to discrimination or individual rights infringement.

– it should comply with precise standards (O'Sullivan et al., 2019), i.e., there should be a number of rules implemented by the EU regarding the minimum standards that a robot should necessarily meet in each field in which it operates, not only from a quality point of view but also from a safety perspective. This requirement is also found in the Cyber-resilience Act.

The AI Act proposal addressed some of these topics, but did not explore the issues of explainability and interpretability in crucial fields. In fact, the requirements in the text of the proposal, and in particular in Article 10, do not refer to explainability and interpretability but rather to the information to be provided in the technical documentation regarding the functioning of the AI system.

We believe that it is not wise to use a black-box model, at least in the cases where health and other fundamental rights are at stake, but also in every case in which the economic loss would be prejudicial to the well being of the users(such in case of huge losses which deprive the users of their house - an example could be a robot that makes high-risk investments). Moreover, when personal data are involved, we believe that black-box models are not compliant with GDPR[22].

Despite the fact that strict safety regulations and standards could be provided by the European Union in addition to existing regulations (e.g., in the medical field, rules governing medical devices), due to their inner nature, lifelong learning models should be strictly controlled in every field in which potential harm to human beings could occur, even if this may create some negative externalities on the market. Protecting users (especially patients, minors, and vulnerable groups) should be more important than ensuring the development of new technologies by the industry sector, as that is already reached by academic research and public investments as well. The much-mentioned chilling effects of safety regulations (and the same goes for product liability rules) on technological progress cannot be, therefore, a valid argument to leverage policy-makers.

As far as military appliances or other potentially harmful AI are concerned, a specific and strict control should be provided by the Government, as it is now for dangerous products or for some supercomputers, for which a license is needed and background checks are performed prior to their utilization. Those kinds of AI should never be freely released to the general public, let alone with open-source licenses. For example, if smart robots could use weapons or kill people in other ways, and anybody could build one thanks to its open-source software and the availability of 3D and 4D printers, they could be easily used for a civil war or to perform terrorist attacks, especially if we consider that self-printed plastic weapons

[22] The GDPR compliance of machine learning models falls outside the scope of this article and will be explored in a separate text in the upcoming months. The issue of interpretability and explainability is explored in further details in the forthcoming book chapter "Legal aspects of AI in the biomedical field. The role of interpretable models".

are not detectable by metal detectors[23] (Falletti, 2022). This risk should be taken seriously by policy-makers of countries where the gun-control laws are less restrictive.

With regards to the mandatory testing, update, and security patches, provided to minimize the risks of a cyberattack, there should be strict checks and audits from States. For the potential harmful devices, such as robots that perform surgery, there should be a mandatory registration at the EU level.

Considering all of the above, as far as machine learning is concerned, we advocate the need for a specific regulation at the European level. Existing rules are not adequate to regulate all the complex issues that could arise from the release into the market of such technologies. In particular, in view of the heterogeneous nature of machine learning-based technologies, and the sectoral nature of their concrete application, it would not be possible to create all-inclusive legislation, but it would be appropriate to regulate each sector separately. It would be possible to emphasize the specificities of each sector (diagnostic, surgical, automotive, educational, etc.) and adapt the regulations accordingly.

As noted by Amidei as early as in 2018, the delay in adopting new regulations in response to market requests could have huge costs and risks of having to accept and adapt to non-fair hetero-determinate rules, as well as it could lead to the risks of having uneven regulations between those Member States that would be quicker in developing new rules on AI (Amidei, 2017).

Unfortunately, the proposals for an European AI Act and for a Cyber-resilience Act fail to give a satisfactory solution to regulate smart robots, as it does not take into consideration the many differences across fields.

3.2. Security rules and standards for producers and programmers

Forcing manufacturers to update their dismissed software as new threats are discovered would move the burden on a single company instead of on millions of citizens, but it is not always possible. For instance, this type of approach could force a company to keep an employee only because he or she is the only person who knows the obsolete programming language, or to invest resources in developing a security patch that is in use in only one type of machine. One corrective measure could be to provide compulsory professional training for employees (similar to that required for the regulated professions in Italy according to D.p.r. no. 137/2012) in order to teach them old or exotic programming languages and to update the obsolete technology. However, in some cases, this is not a satisfactory solution because the code is too complicated (e.g., airplanes avionics:

[23] In fact, even in countries where gun control is less strict, law-makers have tried to put a ban on self-printed weapons, as explained in the press and in our article "Ethical and legal limits to the diffusion of self-produced autonomous weapons": https://www.markey.senate.gov/news/press-releases/senator-markey-rep-meng-lead-colleagues-in-urging-biden-to-roll-back-trumps-deregulation-of-3d-printed-ghost-guns

to be fully operational, a F-35 fighter aircraft requires a software whose source code is 24 million lines long[24]). In some other cases, the law could force the producer to replace, whenever possible, the old and obsolete code with a newer one, thus eliminating part of the obsolescence problem; in fact, the decision to discard a technology and to stop the release of security updates is often left to the producer's discretion, even when the negative impact of a security breach weighs on consumers. The same remarks can be made about the security solutions that could prevent a large number of cyber attacks but that are not mandatory for IoT products, such as the obligation to update devices' software, passwords, and firmware, the obligation to change the default username and password and the requirement of using a unique password for each IoT devices.

Adopting this type of approach could change part of our economy, maybe slowing down technological progress, but also having a good impact on sustainability, as the obsolescence of smart products would probably require a longer time.

A recent case that highlights the need for a regulatory solution that would force programmers to update their software is the CVE-2018-13379 Fortinet vulnerability, which has been reported to the company in 2018[25], but has not been patched until May last year. It has been found that, if the secure sockets layer (SSL) virtual private networking (VPN) service is enabled, attackers can obtain the credentials of logged-in users exploiting the path traversal vulnerability to download FortiOS system files remotely, and no authentication is required. A list of more than 49,000 internet-reachable Fortinet FortiGate VPN systems has just been published on the web, making them vulnerable to attackers.

Regarding the cybersecurity of devices, a first step in the right direction has been made by providing a common certification system in the Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA, even if art. 56 states that "cybersecurity certification shall be voluntary". Providing compulsory certification at the European level and a penalty system in case of non-compliance could have been a great instrument to fight cyber-threats.

Another solution could be to force producers to use open-source software provided and implemented by the EU, from a fair data perspective. There are many reasons why open-source is a good choice. The first is that bugs are easily and quickly detected and security patches can be developed faster because multiple programmers located in different Member States (with different knowledge) are working at it simultaneously. In addition, if the software is not developed by the device producers, the liability regarding bugs cannot be attributed to them, not even under the product liability regulations, but it could be borne by the Member States.

---

24 The problem is well explained at https://spectrum.ieee.org/f35-program-continues-to-struggle-with-software

25 This is explained in more details in the blog of the company that discovered the flaw: https://blog.orange.tw/2019/08/attacking-ssl-vpn-part-2-breaking-the-fortigate-ssl-vpn.html

3.3. Security and standards for users

If the State put a ban on obsolete technology (a kind of "planned obsolescence") to prevent the use of outdated devices that could be hacked, due to a lack of its own risk knowledge and the precautionary principle (Zech, 2021), it is transferring the burden on its citizens, thus forcing each of them to bear the costs of replacing their devices in order to avoid penalties and liability. This means that, for example, a car renting company that has a fleet of autonomous cars could be forced to file for bankruptcy, if unable to invest in non-obsolete machinery. The same goes for a transport company with autonomous trucks, but also for low-income families who rely on a single car.

If, on the contrary, no ban is enacted, but the burden of compliance is still on the backs of the users, there will be a lack of protection for most of them. In fact, even with compulsory insurance system, it is likely that a large number of people would not be properly compensated, as the insurance coverage alone is not so effective (Samu, 2014).

From a cyber-security point of view, it would be dangerous to hold the users accountable for using an unpatched device, mostly because the principle of accountability would not be effective in many cases. The law-abiding attitude is believed to change depending on multiple circumstances, such as personal, cultural, social factors, and even age (Ma, 1985).

In an era in which many people will probably use a robot (e.g., self-driving cars), the risks of having non-updated and unpatched machines circulating, and possibly sold in the black market for those who cannot afford a new product, is too high, especially when those devices could cause personal injuries and death. Self-driving trucks could be hijacked and used for terrorist attacks (Gallese, 2018), harming a great number of people. It is not desirable to let users decide whether to scrap an old truck or not. Furthermore, even if the EU enacted such a system, the cyber-attack risks would still be present in any other country.

In addition, even when ready to abide by the law, average users are not able to detect bias and bugs or to fix them. The most common scenario would be that people who are not familiar with technology would be extremely vulnerable to attacks, without even realizing it. On the other hand, expert users can assemble a home-made robot using different software, even open-source ones, which were published with a different purpose. In this case, the programmer is not responsible for the result of building a robot that operates through some combinations of different software, and the user should be held accountable for it. The same principle should of course be adopted for uses of the robot which are prohibited by the law, explicitly excluded by the producer, or not allowed by the license.

3.4. A balanced system of security and standards

The burden of safety and security regulations should be balanced by law between manufacturers, users and States since some remedies are too expensive and difficult to reach for users or producers, but others are within their reach.

Once the threat is detected through constant security checks, based on the degree of the risks, the Ministry could issue different regulations and force consumers, manufacturers, or even the public authority to comply, depending on the case. For instance, if a colour adversarial patch is placed on an advertisement board on the highway and it constitutes an immediate threat to road safety, there would not be enough time for the manufacturer to create a software update (if ever possible), so it could be the Mayor's responsibility to order the removal within a few hours and to close the road to traffic.

On the other hand, once provided compulsory update developing by producers, it could be the user's responsibility to uninstall outdated software and replace it with a new one, whenever possible, or to bring the robot to technical inspections on a regular basis. The responsibility of the manufacturer could be residual, for the cases over which nor the user nor the State have control.

This solution is not very different from how other safety regulations work: if a new law or emergency decree is introduced to avoid a health threat, sometimes the onus to comply is on the user (for example, anti-abandonment car seat technology in Italy), sometimes it is on the manufacturer (the withdrawal of food from the market according to art. 19 of Regulation (EC) no. 178/2002). State funding and other benefits can also be provided to help both producers and users to bear the costs of compliance.

Particular attention should be paid when there could be a danger to democracy, such in case of national security (Allen & Chan, 2017) or elections. The devices used for those purposes should always have a separate and stricter discipline and the control of them should be the responsibility of the State. We do not believe that any tool involved to some extent in the democratic process should be let in the hands of private companies[26], especially in an era in which democracy is already threatened by the misuse of personal (big) data, social media and fake news (Manheim & Kaplan, 2019; Persily, 2017; Heawood, 2018; Helbing et al., 2019).

Safety and security rules should be implemented also to prevent producers from releasing to the market lifelong learning products that can be dangerous or to allow them only under certain conditions (compulsory insurance and license, registration, etc.).

The opinion according to which human supervision should be always present is entirely acceptable, however, it should be taken into account that the more technology is integrated into everyday life, the more humans tend to rely on it without thinking and actually playing the supposed supervisory role, a phenomenon that is called "automation bias".

[26] This includes the possibility of sharing political content and advertisements through social media, smartphone apps and home devices whose algorithms are based on AI and are profiling users to influence their behaviour. The Cambridge Analytica scandal highlighted the urgent need for a regulatory solution for those AI models that can have an impact on democracy.

4. The Cyber-resilience Act framework

The new framework created by the Cyber-resilience Act proposal is limited, since it is not specific for AI systems or robots, and it excludes from its scope the domain of medical device, automated cars, and drones. However, it represents an important step towards the developing of a safe and secure market for devices with digital elements.

The main requirements found in the Annexes prescribe that such devices must comply with a number of requirements, such as:

– including a secure by default configuration and the possibility of factory reset;

– including measures to protect the device from unauthorized access;

– extending the measures for ensuring the confidentiality and integrity of data to non-personal data;

– extending the adequacy, purpose limitation and data minimization principles to non-personal data;

– implementing cyber-resilience measures to preserve the essential functions of devices;

– minimizing the impact on the availability of services provided by other devices or networks;

– limit in gattack surface;

– implementing appropriate exploitation mitigation mechanisms and techniques to reduce the impact of incidents;

– keep in glogs;

– provide security updates for 5 years.

Similarly to the AI Act, the new proposal also provides for a detailed list of requirements, such as keeping technical documentation, providing information to users, and performing a risk assessment.

A special derogation is foreseen for beta products: “Member States shall not prevent the making available of unfinished software which does not comply with this Regulation provided that the software is only made available for a limited period required for testing purposes and that a visible sign clearly indicates that it does not comply with this Regulation and will not be available on the market for purposes other than testing”. Although not explicitly mentioned in the core text of the proposal, this provision can be extended to devices developed for research purposes.

Recital 10 clarifies that “In order not to hamper innovation or research, free and open-source software developed or supplied outside the course of a commercial activity should not be covered by this Regulation. This is in particular the case for software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable. In the context of software, a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services, by providing a software platform through which the manufacturer monetises other

services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software".

However, the definition of "making available on the market" refers also to devices made available free of charge: "[making available on the market] means any supply of a product with digital elements for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge", therefore researchers collaborating with industry should be very careful.

Conclusion

The road to reach a complete and harmonized regulation of robots in Europe is still a long way to go, considering that AI is evolving very fast and it covers many types of devices that can be employed in many different fields of our lives. Each field has its own peculiarity, hence it is desirable that, together with the general "AI Act" and "Cyber-resilience Act", many different legal instruments, policies, guidelines, standards, covering each a different sector, are enacted.

The first step towards a comprehensive harmonized AI discipline, through the Cyber-resilience Act and its safety and security regulatory framework, is providing for the minimum technical standards that an AI device should meet before being put in the EU market. Preventing cyber-attacks in the most important fields and protecting the fundamental rights of citizens should be the main concern for lawmakers. The AI Act and the Cyber-resilience Act represent a first step towards this direction; however their general principles are not sufficiently detailed to guide programmers on how to implement them in practice.

Policy-makers, after having implemented all relevant standards and technical regulations to ensure that only safe and secure products are released to the market, should carefully assess in what cases lifelong learning models should be allowed to the market, and, where appropriate, leaving part of technological progress as a prerogative of scientific research and public institutions monitored by the Member States at a central level, in particular in case of dangerous products.

For machine learning-based robots, a specific technical regulation at the European level is needed since existing rules are not adequate to regulate all the issues that could occur after the release into the market of such devices. In particular, considering the variety of such technologies, each sector should have distinct rules. The costs and risks deriving from the delay in adopting new regulations in response to market requests should be taken into account as well.

References

Aladin, D., Varlamov, O., Chuvikov, D., Chernenkiy, V., Smelkova, E., & Baldin, A. (2019). Logic-based artificial intelligence in systems for monitoring the enforcing traffic regulations. In *IOP Conference Series: Materials Science and Engineering* (Vol. 534, p. 012025). IOP Publishing. https://doi.org/10.1088/1757-899x/534/1/012025

Allen, G., & Chan, T. (2017). *Artificial intelligence and national security*. Belfer Center for Science and International Affairs Cambridge, MA.

Ames, H., Mingolla, E., Sohail, A., Chandler, B., Gorchetchnikov, A., L´eveill´e, J., Livitz, G., & Versace, M. (2012). The animat: New frontiers in whole brain modeling. *IEEE pulse*, *3*(1), 47–50. https://doi.org/10.1109/mpul.2011.2175638

Amidei, A. (2017). Robotica intelligente e responsabilit`a: profili e prospettive evolutive del quadro normativo europeo. In U. Ruffolo (ed.), *Intelligenza Artificiale e responsabilit`a, Responsabilit`a Comunicazione Impresa* (Vol. 20, Giuffr`e Editore, pp. 63–106).

Barreno, M., Nelson, B., Joseph, A. D., & Tygar, J. D. (2010). The security of machine learning. *Machine Learning, 81*(2), 121–148. https://doi.org/10.1007/s10994-010-5188-5

Bekey, G. A. (2012). Current trends in robotics: Technology and ethics. In *Robot ethics: the ethical and social implications of robotics* (pp. 17–34). The MIT Press, Cambridge.

Bertolini, A. (2013). Robots as products: the case for a realistic analysis of robotic applications and liability rules. *Law, Innovation and Technology*, *5*(2), 214–247. https://doi.org/10.5235/17579961.5.2.214

Bi, S. (2020). Intelligent system for English translation using automated knowledge base. *Journal of Intelligent & Fuzzy Systems*, *39*(4), 5057–5066. https://doi.org/10.3233/jifs-179991

Botros, N. M., & Abdul-Aziz, M. (1994). Hardware implementation of an artificial neural network using field programmable gate arrays (FPGA's). *IEEE Transactions on Industrial Electronics*, *41*(6), 665–667. https://doi.org/10.1109/41.334585

Buchanan, B. (2016). The life cycles of cyber threats. *Survival*, *58*(1), 39–58. https://doi.org/10.1080/00396338.2016.1142093

Chakkravarthy, R. (2019). Artificial intelligence for construction safety. *Professional Safety*, *64*(1), 46.

Chakraborti, T., Kulkarni, A., Sreedharan, S., Smith, D. E., & Kambhampati, S. (2021). Explicability? Legibility? Predictability? Transparency? Privacy? Security? The Emerging Landscape of Interpretable Agent Behavior. *Proceedings of the International Conference on Automated Planning and Scheduling*, *29*, 86–96. https://doi.org/10.1609/icaps.v29i1.3463

Das, S., Dey, A., Pal, A., & Roy, N. (2015). Applications of artificial intelligence in machine learning: review and prospect. *International Journal of Computer Applications*, *115*(9), 31–41. https://doi.org/10.5120/20182-2402

De Swarte, T., Boufous, O., & Escalle, P. (2019). Artificial intelligence, ethics and human values: the cases of military drones and companion robots. *Artificial Life and Robotics*, *24*(3), 291–296. https://doi.org/10.1007/s10015-019-00525-1

Demir, K. A., Döven, G., & Sezen, B. (2019). Industry 5.0 and Human-Robot Co-working. *Procedia Computer Science*, *158*, 688–695. https://doi.org/10.1016/j.procs.2019.09.104

Dietterich, T. G., & Kong, E. B. (1995). *Machine learning bias, statistical bias, and statistical variance of decision tree algorithms*. Technical report, Department of Computer Science, Oregon State University.

Dijkstra, E. W. (1982). Selected writings on computing: a personal perspective. Springer Science & Business Media.

Ebers, M., & Navas, S. (2020). *Algorithms and Law*. Cambridge University Press.

European Parliament. (2017). *European Parliament resolution of 16 February 2017 with recommendations to the commission on civil law rules on robotics* (2015/2103(INL)).

Falletti, E. (2020). Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche. *Il diritto dell'informazione e dell'informatica*, *3*, 169–206.

Funkhouser, K. (2013). Paving the road ahead: autonomous vehicles, products liability, and the need for a new approach. *Utah Law Review*, 437.

Gallese, C. (2018). Prospettive di riforma del diritto internazionale privato giapponese. In M. Cestari, G. Coci, D. Moro, A. Specchio (Eds.), *Orizzonti giapponesi: ricerche, idee, prospettive* (pp. 185–186). Aracne editrice, Roma.

Gilpin, L. H., Bau, D., Yuan, B. Z., Bajwa, A., Specter, M., & Kagal, L. (2018). Explaining Explanations: An Overview of Interpretability of Machine Learning. *2018 IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA)* (pp. 80–89). https://doi.org/10.1109/dsaa.2018.00018

Greene, D., Hoffmann, A. L., & Stark, L. (2019). Better, Nicer, Clearer, Fairer: A Critical Assessment of the Movement for Ethical Artificial Intelligence and Machine Learning. *Proceedings of the Annual Hawaii International Conference on System Sciences*. https://doi.org/10.24251/hicss.2019.258

Haselager, W. F. (2005). Robotics, philosophy and the problems of autonomy. *Cognitive Technologies and the Pragmatics of Cognition*, *13*(3), 515–532. https://doi.org/10.1075/pc.13.3.07has

Heawood, J. (2018). Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal. *Information Polity*, *23*(4), 429–434. https://doi.org/10.3233/ip-180009

Helbing, D., Frey, B. S., Gigerenzer, G., Hafen, E., Hagner, M., Hofstetter, Y., van den Hoven, J., Zicari, R. V., & Zwitter, A. (2018). Will Democracy Survive Big Data and Artificial Intelligence? *Towards Digital Enlightenment*, 73–98. https://doi.org/10.1007/978-3-319-90869-4_7

Hildebrandt, M. (2019). Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning. *Theoretical Inquiries in Law*, *20*(1), 83–121. https://doi.org/10.1515/til-2019-0004

Holzinger, A., Langs, G., Denk, H., Zatloukal, K., & Müller, H. (2019). Causability and explainability of artificial intelligence in medicine. *WIREs Data Mining and Knowledge Discovery*, *9*(4). https://doi.org/10.1002/widm.1312

Ielmini, D., & Ambrogio, S. (2019). Emerging neuromorphic devices. *Nanotechnology*, *31*(9), 092001. https://doi.org/10.1088/1361-6528/ab554b

Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, *62*(1), 15–25. https://doi.org/10.1016/j.bushor.2018.08.004

Lamberton, C., Brigo, D., & Hoy, D. (2017). Impact of robotics, RPA and AI on the insurance industry: challenges and opportunities. *Journal of Financial Perspectives*, *4*(1).

Leenes, R., Palmerini, E., Koops, B. J., Bertolini, A., Salvini, P., & Lucivero, F. (2017). Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues. *Law, Innovation and Technology*, *9*(1), 1–44. https://doi.org/10.1080/17579961.2017.1304921

Lu, H., Li, Y., Chen, M., Kim, H., & Serikawa, S. (2017). Brain Intelligence: Go beyond Artificial Intelligence. *Mobile Networks and Applications*, *23*(2), 368–375. https://doi.org/10.1007/s11036-017-0932-8

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology and Health Care*, *24*(1), 1–9. https://doi.org/10.3233/thc-151102

Ma, H. K. (1985). Cross-Cultural Study of the Development of Law-Abiding Orientation. *Psychological Reports*, *57*(3), 967–974. https://doi.org/10.2466/pr0.1985.57.3.967

Manheim, K. M., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. *Yale Journal of Law and Technology*, *21*, 106–188.

Naur, P., & Randell, B. (Eds.) (1968). *Software Engineering: Report of a conference sponsored by the NATO Science Committee.* Newcastle University.

Nevejans, N. (2016). *European civil law rules in robotics*. Policy Department for Citizens' Rights and Constitutional Affairs.

Nobile, M. S., Vlachou, T., Spolaor, S., Cazzaniga, P., Mauri, G., Pelicci, P. G., & Besozzi, D. (2019). ProCell: Investigating cell proliferation with Swarm Intelligence. *2019 IEEE Conference on Computational Intelligence in Bioinformatics and Computational Biology (CIBCB)* (pp. 1–8). https://doi.org/10.1109/cibcb.2019.8791468

O'Sullivan, S., Nevejans, N., Allen, C., Blyth, A., Leonard, S., Pagallo, U., Holzinger, K., Holzinger, A., Sajid, M. I., & Ashrafian, H. (2019). Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery. *The International Journal of Medical Robotics and Computer Assisted Surgery*, *15*(1), e1968. https://doi.org/10.1002/rcs.1968

Ozkan, B. E., & Bulkan, S. (2019). Hidden Risks to Cyberspace Security from Obsolete COTS Software. *2019 11th International Conference on Cyber Conflict (CyCon)* (pp. 1–19). https://doi.org/10.23919/cycon.2019.8756990

Pan, C., Wang, C. Y., Liang, S. J., Wang, Y., Cao, T., Wang, P., Wang, C., Wang, S., Cheng, B., Gao, A., Liu, E., Watanabe, K., Taniguchi, T., & Miao, F. (2020). Reconfigurable logic and neuromorphic circuits based on electrically tunable two-dimensional homojunctions. *Nature Electronics*, *3*(7), 383–390. https://doi.org/10.1038/s41928-020-0433-9

Pandian, D. A. P. (2019). Artificial intelligence application in smart warehousing environment for automated logistics. *Journal of Artificial Intelligence and Capsule Networks*, *1*(2), 63–72. https://doi.org/10.36548/jaicn.2019.2.002

Papetti, D. M., Spolaor, S., Besozzi, D., Cazzaniga, P., Antoniotti, M., & Nobile, M. S. (2020). On the automatic calibration of fully analogical spiking neuromorphic chips. *2020 International Joint Conference on Neural Networks (IJCNN)*. https://doi.org/10.1109/ijcnn48605.2020.9206654

Persily, N. (2017). Can Democracy Survive the Internet? *Journal of Democracy*, *28*(2), 63–76. https://doi.org/10.1353/jod.2017.0025

Ranjan, A., Janai, J., Geiger, A., & Black, M. (2019). Attacking Optical Flow. *2019 IEEE/CVF International Conference on Computer Vision (ICCV)* (pp. 2404–2413). https://doi.org/10.1109/iccv.2019.00249

Rao, Q., & Frtunikj, J. (2018). Deep learning for self-driving cars. *Proceedings of the 1st International Workshop on Software Engineering for AI in Autonomous Systems* (pp. 35–38). https://doi.org/10.1145/3194085.3194087

Raza, M., Awais, M., Ali, K., Aslam, N., Paranthaman, V. V., Imran, M., & Ali, F. (2020). Establishing effective communications in disaster affected areas and artificial intelligence based detection using social media platform. *Future Generation Computer Systems*, *112*, 1057–1069. https://doi.org/10.1016/j.future.2020.06.040

Richards, N. M., & Smart, W. D. (2016). How should the law think about robots? In R. Calo, M. A. Froomkin, I. Kerr (Eds.), *Robot law*. Edward Elgar.

Roll, I., & Wylie, R. (2016). Evolution and Revolution in Artificial Intelligence in Education. *International Journal of Artificial Intelligence in Education*, *26*(2), 582–599. https://doi.org/10.1007/s40593-016-0110-3

Romanishin, J. W., Gilpin, K., & Rus, D. (2013). M-blocks: Momentum-driven, magnetic modular robots. *2013 IEEE/RSJ International Conference on Intelligent Robots and Systems* (pp. 4288–4295). https://doi.org/10.1109/iros.2013.6696971

Rundo, L., Tangherloni, A., Nobile, M. S., Militello, C., Besozzi, D., Mauri, G., & Cazzaniga, P. (2019). MedGA: A novel evolutionary method for image enhancement in medical imaging systems. *Expert Systems With Applications*, *119*, 387–399. https://doi.org/10.1016/j.eswa.2018.11.013

Samu, S. (2014). The effectiveness of compulsory motor insurance in Zimbabwe. *Journal of Strategic Studies: A Journal of the Southern Bureau of Strategic Studies Trust*, *5*(1), 45–60.

Santosuosso, A., Boscarato, C., & Caroleo, F. (2012). Robot e diritto: una prima ricognizione. *La Nuova Giurisprudenza Commentata*, *494*.

Simoens, P., Mahieu, C., Ongenae, F., De Backere, F., De Pestel, S., Nelis, J., De Turck, F., Elprama, S. A., Kilpi, K., Jewell, C., & Jacobs, A. (2016). Internet of Robotic Things: Context-Aware and Personalized Interventions of Assistive Social Robots (Short Paper). *2016 5th IEEE International Conference on Cloud Networking (Cloudnet)* (pp. 204–207). https://doi.org/10.1109/cloudnet.2016.27

Smith, B. Walker (2016). Lawyers and engineers should speak the same robot language. In R. Calo, M. A. Froomkin, I. Kerr (Eds.), *Robot law* (pp. 78–101). Edward Elgar Publishing.

Sourdin, T. (2018). Judge v Robot? Artificial Intelligence and Judicial Decision-Making. *University of New South Wales Law Journal*, *41*(4), 25167–25177. https://doi.org/10.53637/zgux2213

Wang, W., & Siau, K. (2019). Artificial Intelligence, Machine Learning, Automation, Robotics, Future of Work and Future of Humanity. *Journal of Database Management*, *30*(1), 61–79. https://doi.org/10.4018/jdm.2019010104

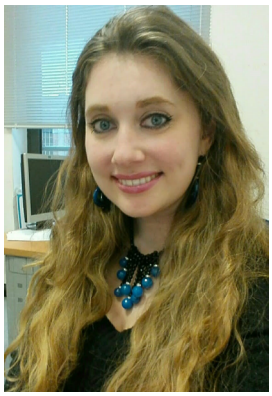
Yano, K. (2017). How artificial intelligence will change HR. *People & Strategy*, *40*(3), 42–47.

Yuniarthe, Y. (2017). Application of Artificial Intelligence (AI) in Search Engine Optimization (SEO). In *2017 International Conference on Soft Computing, Intelligent System and Information Technology (ICSIIT)* (pp. 96–101). https://doi.org/10.1109/icsiit.2017.15

Zech, H. (2021). Liability for AI: public policy considerations. *ERA Forum*, *22*(1), 147–158. https://doi.org/10.1007/s12027-020-00648-0

Zhang, X., Upton, O., Beebe, N. L., & Choo, K. K. R. (2020). IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers. *Forensic Science International: Digital Investigation*, *32*, 300926. https://doi.org/10.1016/j.fsidi.2020.300926

Author information



Chiara Gallese Nobile – PhD, Researcher (postdoc) of research data management, Eindhoven University of Technology (Eindhoven, the Netherlands), Researcher (postdoc) of the Department of Mathematics and Geosciences at the University of Trieste (Trieste, Italy).
Address: P/O 513 5600 MB Eindhoven, the Netherlands
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57222726276
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/AGE-9594-2022
ORCID ID: https://orcid.org/0000-0001-8194-0261
Google Scholar ID: https://scholar.google.com/citations?user=Vmoen8UAAAAJ

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research has been funded by the UNI 4 JUSTICE project.

Article history

Date of receipt – October 13, 2022
Date of approval – November 4, 2022
Date of acceptance – March 6, 2023
Date of online placement – March 10, 2023

Научная статья
УДК 34:004.8:007.524:62-529.4
EDN: https://elibrary.ru/unsonv
DOI: https://doi.org/10.21202/jdtl.2023.2

Регулирование умных роботов и искусственного интеллекта в Европейском союзе

Кьяра Галлезе-Нобиле

Эйндховенский технологический университет
г. Эйндховен, Королевство Нидерландов;
Университет Триеста
г. Триест, Итальянская Республика

Ключевые слова

Европейский союз,
законодательство,
искусственный интеллект,
кибербезопасность,
машинное обучение,
право,
регулирование,
робот,
робототехника,
цифровые технологии

Аннотация

Цель: в последние годы в Европе стала очевидной необходимость создания нормативных актов в области робототехники и искусственного интеллекта. Европейский союз нуждается в стандартизации регулирования, которое обеспечило бы высокий уровень безопасности робототехнических систем и предотвратило потенциальные нарушения. Поэтому новое законодательство должно гарантировать, что именно производители несут ответственность за выявление «слепых зон» в этих системах, содержащих недоработки, а в случае обнаружения уязвимостей на поздних этапах – обновлять систему, даже если модель уже не находится на рынке. Цель данной статьи – предложить ряд возможных поправок к существующим положениям нормативных актов Евросоюза.

Методы: используя методологию Кестемонта для юридических исследований, автор анализирует и сравнивает тексты нормативных актов и увязывает их с техническими положениями об умных роботах, в результате выделяя критические элементы, требующие доработки.

Результаты: в статье предлагаются поправки к существующим проектам законов: по мнению автора, хотя закон об искусственном интеллекте и закон о киберустойчивости представляют собой первый шаг в этом направлении, их основные принципы недостаточно детализированы, а значит, не позволяют регулировать их практическое применение. Поэтому законодатели должны тщательно определить, в каких случаях модели, использующие обучение в течение всего жизненного цикла, могут быть допущены на рынок. Автор предлагает

увеличить сроки обязательного обновления систем, предусмотренные в существующих проектах законов, поскольку пятилетний срок не соответствует уровню риска, связанного с продуктами длительного пользования, такими как транспортные средства.

Научная новизна: автор рассматривает действующую нормативную базу в области систем искусственного интеллекта и устройств с цифровыми элементами, выделяет риски действующей правовой базы и вносит предложения по возможному усовершенствованию существующих проектов законов.

Практическая значимость: материалы статьи могут быть использованы для доработки существующих проектов закона об искусственном интеллекте и закона о киберустойчивости.

Для цитирования

Галлезе-Нобиле, К. (2023). Регулирование умных роботов и искусственного интеллекта в Европейском союзе. *Journal of Digital Technologies and Law*, *1*(1), 33–61. https://doi.org/10.21202/jdtl.2023.2

Список литературы

Aladin, D., Varlamov, O., Chuvikov, D., Chernenkiy, V., Smelkova, E., & Baldin, A. (2019). Logic-based artificial intelligence in systems for monitoring the enforcing traffic regulations. In *IOP Conference Series: Materials Science and Engineering* (Vol. 534, p. 012025). IOP Publishing. https://doi.org/10.1088/1757-899x/534/1/012025

Allen, G., & Chan, T. (2017). *Artificial intelligence and national security*. Belfer Center for Science and International Affairs Cambridge, MA.

Ames, H., Mingolla, E., Sohail, A., Chandler, B., Gorchetchnikov, A., L´eveill´e, J., Livitz, G., & Versace, M. (2012). The animat: New frontiers in whole brain modeling. *IEEE pulse*, *3*(1), 47–50. https://doi.org/10.1109/mpul.2011.2175638

Amidei, A. (2017). Robotica intelligente e responsabilit`a: profili e prospettive evolutive del quadro normativo europeo. In U. Ruffolo (ed.), *Intelligenza Artificiale e responsabilit`a, Responsabilit`a Comunicazione Impresa* (Vol. 20, Giuffr`e Editore, pp. 63–106).

Barreno, M., Nelson, B., Joseph, A. D., & Tygar, J. D. (2010). The security of machine learning. *Machine Learning, 81*(2), 121–148. https://doi.org/10.1007/s10994-010-5188-5

Bekey, G. A. (2012). Current trends in robotics: Technology and ethics. In *Robot ethics: the ethical and social implications of robotics* (pp. 17–34). The MIT Press, Cambridge.

Bertolini, A. (2013). Robots as products: the case for a realistic analysis of robotic applications and liability rules. *Law, Innovation and Technology*, *5*(2), 214–247. https://doi.org/10.5235/17579961.5.2.214

Bi, S. (2020). Intelligent system for English translation using automated knowledge base. *Journal of Intelligent & Fuzzy Systems*, *39*(4), 5057–5066. https://doi.org/10.3233/jifs-179991

Botros, N. M., & Abdul-Aziz, M. (1994). Hardware implementation of an artificial neural network using field programmable gate arrays (FPGA's). *IEEE Transactions on Industrial Electronics*, *41*(6), 665–667. https://doi.org/10.1109/41.334585

Buchanan, B. (2016). The life cycles of cyber threats. *Survival*, *58*(1), 39–58. https://doi.org/10.1080/00396338.2016.1142093

Chakkravarthy, R. (2019). Artificial intelligence for construction safety. *Professional Safety*, *64*(1), 46.

Chakraborti, T., Kulkarni, A., Sreedharan, S., Smith, D. E., & Kambhampati, S. (2021). Explicability? Legibility? Predictability? Transparency? Privacy? Security? The Emerging Landscape of Interpretable Agent Behavior. *Proceedings of the International Conference on Automated Planning and Scheduling*, *29*, 86–96. https://doi.org/10.1609/icaps.v29i1.3463

Das, S., Dey, A., Pal, A., & Roy, N. (2015). Applications of artificial intelligence in machine learning: review and prospect. *International Journal of Computer Applications*, *115*(9), 31–41. https://doi.org/10.5120/20182-2402

De Swarte, T., Boufous, O., & Escalle, P. (2019). Artificial intelligence, ethics and human values: the cases of military drones and companion robots. *Artificial Life and Robotics*, *24*(3), 291–296. https://doi.org/10.1007/s10015-019-00525-1

Demir, K. A., Döven, G., & Sezen, B. (2019). Industry 5.0 and Human-Robot Co-working. *Procedia Computer Science*, *158*, 688–695. https://doi.org/10.1016/j.procs.2019.09.104

Dietterich, T. G., & Kong, E. B. (1995). *Machine learning bias, statistical bias, and statistical variance of decision tree algorithms*. Technical report, Department of Computer Science, Oregon State University.

Dijkstra, E. W. (1982). Selected writings on computing: a personal perspective. Springer Science & Business Media.

Ebers, M., & Navas, S. (2020). *Algorithms and Law*. Cambridge University Press.

European Parliament. (2017). *European Parliament resolution of 16 February 2017 with recommendations to the commission on civil law rules on robotics* (2015/2103(INL)).

Falletti, E. (2020). Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche. *Il diritto dell'informazione e dell'informatica 3*, 169–206.

Funkhouser, K. (2013). Paving the road ahead: autonomous vehicles, products liability, and the need for a new approach. *Utah Law Review*, 437.

Gallese, C. (2018). Prospettive di riforma del diritto internazionale privato giapponese. In M. Cestari, G. Coci, D. Moro, A. Specchio (Eds.), *Orizzonti giapponesi: ricerche, idee, prospettive* (pp. 185–186). Aracne editrice, Roma.

Gallese C. (2023). Legal aspects of AI models in medicine. The role of interpretability. Big Data Analysis and Artificial Intelligence for Medical Science, Wiley

Gilpin, L. H., Bau, D., Yuan, B. Z., Bajwa, A., Specter, M., & Kagal, L. (2018). Explaining Explanations: An Overview of Interpretability of Machine Learning. *2018 IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA)* (pp. 80–89). https://doi.org/10.1109/dsaa.2018.00018

Greene, D., Hoffmann, A. L., & Stark, L. (2019). Better, Nicer, Clearer, Fairer: A Critical Assessment of the Movement for Ethical Artificial Intelligence and Machine Learning. *Proceedings of the Annual Hawaii International Conference on System Sciences*. https://doi.org/10.24251/hicss.2019.258

Haselager, W. F. (2005). Robotics, philosophy and the problems of autonomy. *Cognitive Technologies and the Pragmatics of Cognition*, *13*(3), 515–532. https://doi.org/10.1075/pc.13.3.07has

Heawood, J. (2018). Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal. *Information Polity*, *23*(4), 429–434. https://doi.org/10.3233/ip-180009

Helbing, D., Frey, B. S., Gigerenzer, G., Hafen, E., Hagner, M., Hofstetter, Y., van den Hoven, J., Zicari, R. V., & Zwitter, A. (2018). Will Democracy Survive Big Data and Artificial Intelligence? *Towards Digital Enlightenment*, 73–98. https://doi.org/10.1007/978-3-319-90869-4_7

Hildebrandt, M. (2019). Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning. *Theoretical Inquiries in Law*, *20*(1), 83–121. https://doi.org/10.1515/til-2019-0004

Holzinger, A., Langs, G., Denk, H., Zatloukal, K., & Müller, H. (2019). Causability and explainability of artificial intelligence in medicine. *WIREs Data Mining and Knowledge Discovery*, *9*(4). https://doi.org/10.1002/widm.1312

Ielmini, D., & Ambrogio, S. (2019). Emerging neuromorphic devices. *Nanotechnology*, *31*(9), 092001. https://doi.org/10.1088/1361-6528/ab554b

Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, *62*(1), 15–25. https://doi.org/10.1016/j.bushor.2018.08.004

Lamberton, C., Brigo, D., & Hoy, D. (2017). Impact of robotics, RPA and AI on the insurance industry: challenges and opportunities. *Journal of Financial Perspectives*, *4*(1).

Leenes, R., Palmerini, E., Koops, B. J., Bertolini, A., Salvini, P., & Lucivero, F. (2017). Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues. *Law, Innovation and Technology*, *9*(1), 1–44. https://doi.org/10.1080/17579961.2017.1304921

Lu, H., Li, Y., Chen, M., Kim, H., & Serikawa, S. (2017). Brain Intelligence: Go beyond Artificial Intelligence. *Mobile Networks and Applications*, *23*(2), 368–375. https://doi.org/10.1007/s11036-017-0932-8

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology and Health Care*, *24*(1), 1–9. https://doi.org/10.3233/thc-151102

Ma, H. K. (1985). Cross-Cultural Study of the Development of Law-Abiding Orientation. *Psychological Reports*, *57*(3), 967–974. https://doi.org/10.2466/pr0.1985.57.3.967

Manheim, K. M., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. *Yale Journal of Law and Technology*, *21*, 106–188.

Naur, P., & Randell, B. (Eds.) (1968). *Software Engineering: Report of a conference sponsored by the NATO Science Committee.* Newcastle University.

Nevejans, N. (2016). *European civil law rules in robotics*. Policy Department for Citizens' Rights and Constitutional Affairs.

Nobile, M. S., Vlachou, T., Spolaor, S., Cazzaniga, P., Mauri, G., Pelicci, P. G., & Besozzi, D. (2019). ProCell: Investigating cell proliferation with Swarm Intelligence. *2019 IEEE Conference on Computational Intelligence in Bioinformatics and Computational Biology (CIBCB)* (pp. 1–8). https://doi.org/10.1109/cibcb.2019.8791468

O'Sullivan, S., Nevejans, N., Allen, C., Blyth, A., Leonard, S., Pagallo, U., Holzinger, K., Holzinger, A., Sajid, M. I., & Ashrafian, H. (2019). Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery. *The International Journal of Medical Robotics and Computer Assisted Surgery*, *15*(1), e1968. https://doi.org/10.1002/rcs.1968

Ozkan, B. E., & Bulkan, S. (2019). Hidden Risks to Cyberspace Security from Obsolete COTS Software. *2019 11th International Conference on Cyber Conflict (CyCon)* (pp. 1–19). https://doi.org/10.23919/cycon.2019.8756990

Pan, C., Wang, C. Y., Liang, S. J., Wang, Y., Cao, T., Wang, P., Wang, C., Wang, S., Cheng, B., Gao, A., Liu, E., Watanabe, K., Taniguchi, T., & Miao, F. (2020). Reconfigurable logic and neuromorphic circuits based on electrically tunable two-dimensional homojunctions. *Nature Electronics*, *3*(7), 383–390. https://doi.org/10.1038/s41928-020-0433-9

Pandian, D. A. P. (2019). Artificial intelligence application in smart warehousing environment for automated logistics. *Journal of Artificial Intelligence and Capsule Networks*, *1*(2), 63–72. https://doi.org/10.36548/jaicn.2019.2.002

Papetti, D. M., Spolaor, S., Besozzi, D., Cazzaniga, P., Antoniotti, M., & Nobile, M. S. (2020). On the automatic calibration of fully analogical spiking neuromorphic chips. *2020 International Joint Conference on Neural Networks (IJCNN)*. https://doi.org/10.1109/ijcnn48605.2020.9206654

Persily, N. (2017). Can Democracy Survive the Internet? *Journal of Democracy*, *28*(2), 63–76. https://doi.org/10.1353/jod.2017.0025

Ranjan, A., Janai, J., Geiger, A., & Black, M. (2019). Attacking Optical Flow. *2019 IEEE/CVF International Conference on Computer Vision (ICCV)* (pp. 2404–2413). https://doi.org/10.1109/iccv.2019.00249

Rao, Q., & Frtunikj, J. (2018). Deep learning for self-driving cars. *Proceedings of the 1st International Workshop on Software Engineering for AI in Autonomous Systems* (pp. 35–38). https://doi.org/10.1145/3194085.3194087

Raza, M., Awais, M., Ali, K., Aslam, N., Paranthaman, V. V., Imran, M., & Ali, F. (2020). Establishing effective communications in disaster affected areas and artificial intelligence based detection using social media platform. *Future Generation Computer Systems*, *112*, 1057–1069. https://doi.org/10.1016/j.future.2020.06.040

Richards, N. M., Smart, W. D. (2016). How should the law think about robots? In R. Calo, M. A. Froomkin, I. Kerr (Eds.), *Robot law*. Edward Elgar.

Roll, I., & Wylie, R. (2016). Evolution and Revolution in Artificial Intelligence in Education. *International Journal of Artificial Intelligence in Education*, *26*(2), 582–599. https://doi.org/10.1007/s40593-016-0110-3

Romanishin, J. W., Gilpin, K., & Rus, D. (2013). M-blocks: Momentum-driven, magnetic modular robots. *2013 IEEE/RSJ International Conference on Intelligent Robots and Systems* (pp. 4288–4295). https://doi.org/10.1109/iros.2013.6696971

Rundo, L., Tangherloni, A., Nobile, M. S., Militello, C., Besozzi, D., Mauri, G., & Cazzaniga, P. (2019). MedGA: A novel evolutionary method for image enhancement in medical imaging systems. *Expert Systems With Applications*, *119*, 387–399. https://doi.org/10.1016/j.eswa.2018.11.013

Samu, S. (2014). The effectiveness of compulsory motor insurance in Zimbabwe. *Journal of Strategic Studies: A Journal of the Southern Bureau of Strategic Studies Trust*, *5*(1), 45–60.

Santosuosso, A., Boscarato, C., & Caroleo, F. (2012). Robot e diritto: una prima ricognizione. *La Nuova Giurisprudenza Commentata*, *494*.

Simoens, P., Mahieu, C., Ongenae, F., De Backere, F., De Pestel, S., Nelis, J., De Turck, F., Elprama, S. A., Kilpi, K., Jewell, C., & Jacobs, A. (2016). Internet of Robotic Things: Context-Aware and Personalized Interventions of Assistive Social Robots (Short Paper). *2016 5th IEEE International Conference on Cloud Networking (Cloudnet)* (pp. 204–207). https://doi.org/10.1109/cloudnet.2016.27

Smith, B. Walker (2016). Lawyers and engineers should speak the same robot language. In R. Calo, M. A. Froomkin, I. Kerr (Eds.), *Robot law* (pp. 78–101). Edward Elgar Publishing.

Sourdin, T. (2018). Judge v Robot? Artificial Intelligence and Judicial Decision-Making. *University of New South Wales Law Journal*, *41*(4), 25167–25177. https://doi.org/10.53637/zgux2213

Wang, W., & Siau, K. (2019). Artificial Intelligence, Machine Learning, Automation, Robotics, Future of Work and Future of Humanity. *Journal of Database Management*, *30*(1), 61–79. https://doi.org/10.4018/jdm.2019010104

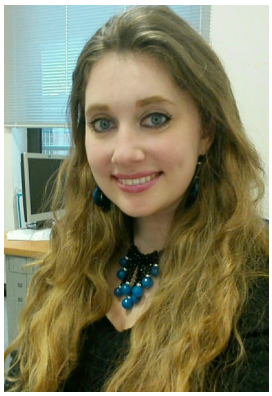
Yano, K. (2017). How artificial intelligence will change HR. *People & Strategy*, *40*(3), 42–47.

Yuniarthe, Y. (2017). Application of Artificial Intelligence (AI) in Search Engine Optimization (SEO). In *2017 International Conference on Soft Computing, Intelligent System and Information Technology (ICSIIT)* (pp. 96–101). https://doi.org/10.1109/icsiit.2017.15

Zech, H. (2021). Liability for AI: public policy considerations. *ERA Forum*, *22*(1), 147–158. https://doi.org/10.1007/s12027-020-00648-0

Zhang, X., Upton, O., Beebe, N. L., & Choo, K. K. R. (2020). IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers. *Forensic Science International: Digital Investigation*, *32*, 300926. https://doi.org/10.1016/j.fsidi.2020.300926

Сведения об авторе



Галлезе-Нобиле Кьяра – доктор наук, научный сотрудник (постдок) по управлению исследовательскими данными, Эйндховенский технологический университет (Эйндховен, Королевство Нидерландов); научный сотрудник (постдок) департамента математики и наук о земле, Университет Триеста (Триест, Итальянская Республика)
Адрес: а/я 513 5600 МБ Эйндховен, Королевство Нидерландов
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57222726276
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/AGE-9594-2022
ORCID ID: https://orcid.org/0000-0001-8194-0261
Google Scholar ID: https://scholar.google.com/citations?user=Vmoen8UAAAAJ

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Финансирование

Исследование выполнено при поддержке проекта UNI 4 JUSTICE.

История статьи

Дата поступления – 13 октября 2022 г.
Дата одобрения после рецензирования – 4 ноября 2022 г.
Дата принятия к опубликованию – 6 марта 2023 г.
Дата онлайн размещения – 10 марта 2023 г.