Research article
DOI: https://doi.org/10.21202/jdtl.2023.13

Legal Aspects of the Use Artificial Intelligence in Telemedicine

Chiara Gallese Nobile

Eindhoven University of Technology
Eindhoven, Netherlands;
University of Trieste
Trieste, Italy

Keywords

Artificial intelligence,
data protection,
digital inequality,
digital technologies,
law,
legislation,
personal data,
private life,
regulation,
telemedicine

Abstract

Objective: the rapid expansion of the use of telemedicine in clinical practice and the increasing use of Artificial Intelligence has raised many privacy issues and concerns among legal scholars. Due to the sensitive nature of the data involved particular attention should be paid to the legal aspects of those systems. This article aimed to explore the legal implication of the use of Artificial Intelligence in the field of telemedicine, especially when continuous learning and automated decision-making systems are involved; in fact, providing personalized medicine through continuous learning systems may represent an additional risk. Particular attention is paid to vulnerable groups, such as children, the elderly, and severely ill patients, due to both the digital divide and the difficulty of expressing free consent.

Methods: comparative and formal legal methods allowed to analyze current regulation of the Artificial Intelligence and set up its correlations with the regulation on telemedicine, GDPR and others.

Results: legal implications of the use of Artificial Intelligence in telemedicine, especially when continuous learning and automated decision-making systems are involved were explored; author concluded that providing personalized medicine through continuous learning systems may represent an additional risk and offered the ways to minimize it. Author also focused on the issues of informed consent of vulnerable groups (children, elderly, severely ill patients).

Scientific novelty: existing risks and issues that are arising from the use of Artificial Intelligence in telemedicine with particular attention to continuous learning systems are explored.

Practical significance: results achieved in this paper can be used for lawmaking process in the sphere of use of Artificial Intelligence in telemedicine and as base for future research in this area as well as contribute to limited literature on the topic.

For citation

Gallese Nobile, C. (2023). Legal Aspects of the Use Artificial Intelligence in Telemedicine. *Journal of Digital Technologies and Law, 1*(2), 314–336. https://doi.org/10.21202/jdtl.2023.13

Contents

Introduction
1. Legal framework regarding Telemedicine in Europe
2. Artificial Intelligence in Telemedicine
3. Continuous learning and personalized medicine
4. Privacy issues in Telemedicine
5. Article 22 GDPR and human oversight
6. Informed Consent
7. Vulnerable groups
8. The balance between privacy and protection from harm at distance
9. AI auditing measures as an additional safeguard
Conclusions
References

Introduction

The term “telemedicine” was coined in the 1970s by Thomas Bird and was defined by Strehle and Shabde as “healing at a distance” (Strehle & Shabde, 2006). A number of official definitions have been added over time, such as: “the provision of healthcare services, through use of ICT, in situations where the health professional and the patient (or two health professionals) are not in the same location. It involves secure transmission of medical data and information, through text, sound, images or other forms needed for the prevention, diagnosis, treatment and follow-up of patients. Telemedicine encompasses a wide variety of services. Those most often mentioned in peer-reviews are teleradiology, telepathology, teledermatology, teleconsultation, telemonitoring, telesurgery and teleophthalmology. Other potential services include call centres/online

information centres for patients, remote consultation/e-visits or videoconferences between health professionals.

Health information portals, electronic health record systems, electronic transmission of prescriptions or referrals (e-prescription, e-referrals) are not regarded as telemedicine services for the purpose of this Communication."[1], which has been used as a reference for national implementation (such as the definition provided by the Italian Ministry in 2012)[2].

This new way of providing health care services is not only useful to optimize processes by making them more efficient, and it is not intended to replace traditional in-patient medicine (Burrai et al., 2021), but it also serves to provide the patient with better follow-up, a greater chance of prevention and greater comfort, especially in the case of disabled or particularly frail patients. In fact, compared to traditional medicine, the devices used to monitor the patient from home allow patients not to travel as often to the hospital or to the doctor's office, remaining comfortably at their residence (which may be their own home, but also hotel, if they fall ill during holidays or business trips). This circumstance is particularly important during the pandemic, as it helps limit the chance of spreading the Sars-cov-2 infection or to get a hospital-acquired infection. It can be said that it was precisely the Covid-19 emergency that gave a boost to the use of medicine, as it sought to ensure continuity of health care even in a context where travel has long been limited.

This incredible opportunity, however, may create some risks, and many legal issues of different nature may arise. In this paper we will focus in particular on the legal issues connected to the use of Artificial Intelligence (AI) in telemedicine, with particular attention to continuous learning systems.

1. Legal Framework Regarding Telemedicine in Europe

The rapid expansion of the use of telemedicine in clinical practice has prompted, for some time now, the European Union to address the implications of the use of new technologies on patients, the development of the e-Health market, the creation of European Health Data Space, and the impact that this may have on the health services of Member States. Therefore, over the years, several soft law instruments have been issued, such as guidelines, recommendations, and other tools, analyzed in detail by Botrugno (Bortugno, 2014). In addition, the European Regulation on Medical Devices, fully applicable as of May 26, 2021, disciplines all telemedicine devices used to make a diagnosis and deliver care at a distance[3]. In Italy as well, the

1 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on telemedicine for the benefit of patients, healthcare systems and society. (2008). https://commission.europa.eu/system/files/2022-10/cwp_2023.pdf

2 Ministero della Salute. Telemedicina – Linee di indirizzo nazionali. (2012). https://www.salute.gov.it/portale/documentazione/p6_2_2_1.jsp?id=2129

3 Regulation (Eu) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745

matter is mainly left to soft law, in particular the Guidelines dating back to 2012[4]. In addition to this, in 2017 Law no. 219 regulated the matter of informed consent and Anticipated Treatment Arrangements in case of possible and future inability to self-determine, a topic that, as will be seen, in the case of telemedicine delivered through intelligent systems takes on particular importance. It has been pointed out, in fact, that if the emotional needs of the patient were to be considered an integral part of the treatment, telemedicine could be qualified only as an integrative service to the traditional ones (Campagna, 2020).

To the current regulatory framework, well examined by Campagna, will soon be added the new European Regulation on AI (AI Act), approved by the European Commission during 2021 (Campagna, 2020). This instrument will bring a very relevant change on AI-based telemedicine devices, as it will impose very stringent requirements for them to be used in medical practice, clinical trials and scientific research. Medical devices, in fact, are classified by the Regulation as "high risk". The new regulation will complement GDPR and MDR, providing for additional guarantees for users (both patients and health care professionals).

2. Artificial Intelligence in Telemedicine

With the progress of technology, many of AI techniques have been applied to telemedicine, with the aim of improving its results, since, in several areas (such as image recognition), the performance of AI has now surpassed that of humans.

However, healthcare professionals are still reticent to use these techniques in clinical practice: data from the research conducted in 2020 on Italian physicians by the Digital Innovation in Healthcare Observatory of the Politecnico di Milano on Connected Care in the Covid-19 emergency showed that only 9% of them used them before the Covid emergency and only 6% work in a facility that introduced (or enhanced) them during the pandemic. Despite this, 60% of medical specialists believe AI techniques can play a key role in emergency situations, 52% believe they help personalize care, 51% believe they help make care more effective, and 50% believe they help reduce the likelihood of clinical errors. Those results are similar to those of other surveys conducted in different countries, where concerns about liability were also raised (Scheetz, 2021). However, surveys shows that the general public has a great distrust over AI models employed in medicine (Castagno & Khalifa, 2020).

Trends in the development of AI use in telemedicine can be classified into four different groups: patient monitoring, health information technology, intelligent diagnostic assistance, and collaboration in information analysis (Pacis et al., 2018).

[4] Ministero della Salute, Telemedicina - Linee di indirizzo nazionali. https://www.salute.gov.it/portale/ehealth/homeEHealth.jsp

The branches of medicine in which these techniques are most frequently used are diabetes care, cardiology, ophthalmology, oncology, epidemiology, and dermatology. During the pandemic, telemedicine has been used, among other things, to help the management of the patients who were suspected to be infected and to provide assistance for chronic diseases (Ye., 2020). Typically, patients wear removable devices such as smart watches or sensors, or use an app on their tablets; however, more invasive methods can also be used, such as pills that can be swallowed, cameras placed inside the home, and sensors that monitor actions such as opening medication packages. Low-intrusive techniques can also be employed, such as the use of an app on the cellphone, especially in the case of younger patients, who may engage in telemedicine through a game (Giunti, 2014), or older patients (Schatten & Protrka, 2021), who need to be stimulated in engaging with the AI systems. Devices using the more complex techniques also adapt to the individual patient, continuing to learn throughout the duration of use. This creates a number of ethical and legal problems, on which doctrine and jurisprudence are trying to conduct an in-depth reflection, in order to suggest guidelines for healthcare professionals and researchers who develop these devices. Very often, in fact, the regulatory framework - as in the case of personal data protection – is complicated even for jurists, a circumstance that represents an obstacle to effective patient protection.

The complex regulatory framework is further complicated by the fragmentation of the AI discipline within the European Union, which the new and ambitious AI Act intends to remedy. Today, however, there remain, and will remain even after the entry into force of this legal instrument, many points peculiar to each Member State in terms of protection of personal data, professional liability of the doctor, informed consent, product liability and criminal liability.

3. Continuous Learning and Personalized Medicine

One of the most popular models to provide personalized medicine is the so-called continuous learning. Physicians want to provide the patient with the best possible care, which also means, in some cases, trying to adjust health care services to a specific patient's needs, due to the differences between ethnicities, genders, habits, family anamnesis, psychological state, etc. This goal can effectively be achieved with the help of AI through systems that learn through use by the patient and adapt to their characteristics over time. From a legal perspective, particular attention should be paid to models based on machine learning, i.e., machine learning (especially deep learning) and also to those that are based on a black-box approach (Rodrigues, 2020; Lakkaraju, 2019), 15 since in these cases the programmers create the model and provide relevant examples, but they do not know the end result because the model is designed to learn on its own (before it is marketed, during the training phase, but also after it is marketed). This often means that it is not possible to know the reason behind the output given by those models, so it is important to explore and understand how they behave in different scenarios (Davis, 2016).

This problem is not limited to telemedicine, but it is related to all AI applications; however, the use of this type of models in the context of telemedicine poses major risks not only because of the category of data involved, but also due to their potential impact on fundamental rights of patients. These systems may be more dangerous in case of telemedicine than they are in case of in presence medicine especially because the patient is not closely monitored by the doctor, being physically away. We will explore these themes in the following. We could consider, as an example, the case of a smart watch employed to monitor diabetes in children, which detect blood levels of sugar, measure physiological values (such as the heartbeat), reminds to eat and exercise, and suggest the correct amount of medicine to be assumed by the patient, communicating the output to the doctor. On the basis of this output, the doctor is able to set appointments, testing, and medical evaluations. In the case of continuous learning, one of the main issues is that neither the programmer nor the physician who will use the AI system can know a priori how it will behave and what it will learn from the interaction with the patient, since it is a system that evolves over time. In fact, four elements should be taken into consideration. The first is that the quality of the training reflects the quality of the samples: if the final user provides the system with biased samples, or samples characterized by poor quality, the behavior of the AI will eventually change to reflect the extended learning set.

One notable example was the case of the Tay chatbot[5]. In the case of personalized telemedicine, many examples are provided directly by the patient through the use of the system. Clearly, the patient is not an expert, and is unable to understand the implications of certain choices. For example, a child may lend the smart watch to classmates or to younger siblings, thus providing inexact measurements to the system. The consequence of an inaccurate observation may lead the system to believe that the child has lower level of sugar in the blood, and then suggest to take less medicine than needed. Even if doctors were present to check the amount of medicine suggested by the system (which would be very unlikely when the medicine must be assumed everyday, due to the costs of an examination on a daily basis), they would not be able to infer that the glucose levels were wrongly influenced by external factors or by a wrongful device management by the patient, unless the device is equipped with a camera that allows to monitor all interactions with the system. In such case, the only technical way to prevent the misuse of the device is to enact strict tele-monitoring measures, which are generally considered invasive of privacy and very intrusive in patients' lives. Even from a liability point of view, there could be doubts regarding the person who is responsible for the error of the system in such cases. Could the producer or programmer be held liable for failing to provide an unsafe device which is lacking of a monitoring mechanism? Is the doctor liable for not noticing the abnormal

[5] The case of Tay, the Microsoft's Twitter bot based on AI, that became racist and nazist. https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter

blood levels? Is the parent/guardian of the child liable for failing to oversee the use of the system? To tackle some of these issues, on September 28, 2022, the European Commission published a proposal for an AI Liability Directive, complementing the EU AI Act, which considers medical devices as «high risk systems», thus subject to stricter requirements. This reform was needed and long advocated by scholars, due to the fact that existing liability rules were inadequate to regulate the use of AI systems and, in particular, machine learning models (Gallese, 2022).

According to the new discipline, there is a presumption of fault for the person who made the system available on the market: as a general rule, the manufacturer or the importer will be liable for the damage produced by the system and "national courts shall presume, for the purposes of applying liability rules to a claim for damages, the causal link between the fault of the defendant and the output produced by the AI system or the failure of the AI system to produce an output». This new rule has two exceptions in case the claimant is able to demonstrate that the user of the system: • "did not comply with its obligations to use or monitor the AI system in accordance with the accompanying instructions of use or, where appropriate, suspend or interrupt its use pursuant to [Article 29 of the AI Act]», or «exposed the AI system to input data under its control which is not relevant in view of the system's intended purpose pursuant to [Article 29(3) of the Act]». The ratio of the rule is to protect users, due to the difficulty of assessing the causal link between the behavior of the system and the incorrect output (especially in case of black boxes).

Under this new discipline, it is difficult to consider doctors liable, both because they are unable to physically influence the system (unless they are provided with full remote control and tele-monitoring measures), and because they are not expert in machine learning techniques to such an extent to be able to correct the way the model is learning. A second element to consider is that machine learning methods are prone to overfitting, i.e., they tend to lose their capability to generalize. This circumstance – well known to machine learning practitioners – is generally detected by observing the relationship between the training error and the test error: when an improvement of the error on the training set leads to a worse error on the test dataset, the network is overfitting and the training process should be stopped. The latter technique – one of the most widespread and effective to prevent overfitting – is known as early stopping and is clearly not applicable in the case of systems that are supposed to be both sold "market ready" (i.e., the learning process was halted before overfitting) and able to learn outside the factory.

In our example, the smart watch may lose its capability to generalize after being used on the patient for a while, both because of an incorrect use or because in that specific time frame the number of specific types of observations were unbalanced (e.g., the patient has been ill for a while, and the heartbeat or the blood analysis have not been normal for a long time). From a legal point of view, this circumstance is relevant not only for the liability of programmers, who will be subject to the new AI liability regime, but also for the new safety and security framework introduced by the AI Act and the proposal for the so-called Cyber-resilience Act. Thirdly, these problems are exacerbated in the case of lifelong continual learning (Parisi, 2019), i.e., machine learning methods that continuously receive new instances to be

used to refine the behavior of the system. As a matter of fact, these methods are challenging because the new samples are often unbalanced (e.g., some categories are more represented than others, due to their probability to be met in the "real world"), a circumstance that can strongly affect the quality of the learning and impact the future behavior of that AI. In the case of the smart watch, it is possible that the specific characteristics of the patients lead to an over-representation of some physiological values, leading to incorrect outcomes.

Finally, the problem is basically not solvable in the extreme case of generalized class incremental learning (Mi, 2020), in which the machine learning method receives new instances that can, in principle, belong to new classes/cases never considered before: in this peculiar situation, the algorithm must be able to reconfigure its internal functioning (e.g., in the case of deep neural networks, adapt the architecture, change the topology, alter the number of neurons, and re-calibrate all parameters) which clearly prevents any realistic possibility of predicting the future behavior of the system. In our example, the patient may have unique characteristics that lead to unusual physiological levels that were not present in the training data sets. In this scenario, it may be dangerous for the patient, as the system suggestions may be wrong and lead to assume an incorrect amount of medicine, and the doctor is not present to correct the error.

The proposal for the AI Act only superficially tackles the issue of continuous learning at article 15: "[...] 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 [...]". Recital 78 adds that "In order to ensure that providers of high-risk AI systems can take into account the experience on the use of high-risk AI systems for improving their systems and the design and development process or can take any possible corrective action in a timely manner, all providers should have a post-market monitoring system in place. This system is also key to ensure that the possible risks emerging from AI systems which continue to 'learn' after being placed on the market or put into service can be more efficiently and timely addressed. In this context, providers should also be required to have a system in place to report to the relevant authorities any serious incidents or any breaches to national and Union law protecting fundamental rights resulting from the use of their AI systems.

This provision is extremely vague and it does not clarify what possible mitigation measures or correcting actions may be considered adequate. The practical implementation of this paragraph will be difficult due to its opacity and it will leave the interpretation open to judicial discretion. The provision of a "post-market monitoring system" is a measure that may be helpful but scarcely effective when referred to personalized medicine, as producers are not able to constantly monitor every single patient. Continuous learning poses a major legal problem in multiple respects (Marchant & Lindor, 2012).

For example, it challenges the traditional liability paradigm: is it possible to adapt a strict liability regime to a situation where neither the programmer nor the manufacturer can predict the behavior of the AI? And from a technical point of view, is it safe to use on patients a product that, even if trained by the manufacturer, cannot be fully explained? Some have theorized a so-called responsibility gap (Matthias, 2004), while others have opposed this view (Tigard, 2020).

In these cases, it becomes really difficult to assume professional liability on the part of the physician. However, many privacy issues arise as well. For example, because the health care professional has no control over the way in which those systems process the patients' health data, they are not able to fully comply with the transparency obligations. We will explore the privacy issues in the next section.

4. Privacy Issues in Telemedicine

One of the most relevant aspects in the field of telemedicine and AI is definitely the protection of personal data and, in particular, the European Regulation No. 679/2016 (GDPR). Under the GDPR, health data, along with a few others, are considered "special categories of data" (Art. 9) and are therefore subject to increased legal protection.

Telemedicine, as well as traditional medicine, involves the processing of special categories of personal data, that is health data. Patients' data employed by AI models in the health care sector can rarely be fully anonymous; most often, they are considered pseudonymized, as the hospital or other health care facility is able to match it back with patients' names and other personal details.

Even when telemedicine devices are not based on AI, the identity of the patients is most of the time known to the health care professionals, as the goal of the system is to provide health care services to a specific individual. GDPR and other privacy law rules (e.g., national implementation acts, sectoral internal laws, etc.), thus, will apply. Because of the ways telemedicine is necessarily carried out, there are a number of privacy issues that will always be present.

The most obvious one is security, as interactions at a distance imply that a connection must be established (between patients and doctors, but also between different professionals). Security measure prescribed by article 32 GDPR must be in place: it must be assured that the connection is secure, that the identity of patients and doctors is ascertained, that all persons involved are adequately trained, and that data are correctly stored and deleted when no longer needed. Especially in cases involving older patients, who are generally not familiar with new technologies, the risk of data breaches is high. IoT devices may be lost, passwords may be cracked by malicious attackers, and data may be deleted by mistake. The fact that the device is in the patient's hand means that the health care professionals and their IT experts are not always present to check the system.

Before introducing these devices, therefore, patients should be adequately trained. However, recent attacks towards hospitals have highlighted that organizational measures implemented by hospitals are not always at the state-of-the-art, mainly due to the lack of proper training of employees, who have a low level of cyber-security awareness (Gioulekas, 2022).

In providing telemedicine services, hospitals and other health care facilities need to make sure that they are able to fulfill the requirements of art. 32 GDPR, which includes training their employees regarding basic cyber-security measures. If health care professional are not able to train themselves regarding security, it is hardly possible that they are able to monitor how patients interact with the system. Because they are not technical experts, they may also be unable to detect anomalies in the system, such as an incorrect training of the neural network. In this context, it is necessary that devices are regularly checked, updated, and re-calibrated by AI experts. Additional safeguards with regards to special categories of data are required by the AI Act in the last paragraph of article 10: it is possible to process them to the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to high-risk AI systems, but appropriate safeguards are necessary (such as technical limitations on the re-use of data, and the use of state-of-the-art technical measures, including pseudonymisation or encryption).

When employing AI system to deliver telemedicine services, privacy by design and by default principles should be carefully implemented in the system, taking into account the data minimization and storage limitation principles as well. To facilitate this, Recital 44 is accounting for an additional specific purpose that may allow the data processing of health data, that is the “bias monitoring, detection and correction”, in order to create a fair and trustworthy AI system.

The above-mentioned requirements can be difficult to implement in the case of continuous learning: how can accuracy, up-to-datedness, and data minimization be ensured, if it is not possible to predict how the system will behave? Another general issue that may arise in telemedicine is the transfer of medical data abroad. The distance between the patient and the doctor may involve cross-border consultation, subject to different jurisdictions.

This problem is unique to tele-medicine, as the medical consultation domain is strictly regulated in every country of the world, providing different rules regarding consent, transparency, quality standards, liability, insurance, data protection, security, identification, contractual relationships, payments, professional ethics, etc. Each of these elements may be the object of a lawsuit or an official investigation, creating conflicts of laws. Some of these aspects can be regulated by contract, but most of all are directly regulated by the foreign law and cannot be waived by contract. If a dispute arises, it would be extremely difficult for the patient, who is already in a position of disadvantage, to seek compensation and obtain legal redress. Even when a contractual arrangement is possible, it may be difficult to reach an agreement regarding responsibilities and liability regarding a system that is unpredictable.

Therefore, the risks involved are exacerbated if compared with an in-person consultation, and the extreme uncertainty regarding the behavior of the system makes it difficult to regulate the relationship between the patient and the doctor. In addition, the device employed to deliver the service may rely to cloud solutions that may have their servers outside EU.

Due to the nature of the data involved, the risks for the patients are higher if compared with a different domain. Although a doctor can store a patient's data in a foreign cloud storage even after a physical consultation, the difference in case of continuous learning devices is that the data are modified and updated in real time, thus giving actual and relevant information to potential attackers, to foreign authorities, and to the manufacturer of the system. In a device that does not collect and make use of data in real time, it is easier for patients to have control over their data, to delete them, to choose what information to store and feed into the model, and to have access to it, as required by the new proposal for the so-called Data Act. A careful assessment is needed before employing those systems, and a Data Protection Impact Assessment (DPIA) may be needed. Appropriate contractual agreement related to data protection may also be needed between the hospital and the processors providing the telemedicine devices.

5. Article 22 GDPR and Human Oversight

The use of AI-based devices in telemedicine often falls under the definition of automated decision-making (ADM) and profiling (Art. 22), for example in the case of automatic scanning of medical imaging to provide a diagnosis. Along with the principle of transparency, which guarantees data subjects the right to be informed about how their data will be used and the consequences of processing on them, the GDPR also guarantees an additional right with regard to ADM and profiling: the right to an explanation. This means that "The controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision without necessarily always attempting a complex explanation of the algorithms used or disclosure of the full algorithm. The information provided should, however, be meaningful to the data subject"[6].

In this context, black box models, and in particular those based on continuous learning, cannot meet this requirement, as it is not possible to justify to the patient why the model has given a certain output. The guidelines note that "Complexity is no excuse for failing to provide information to the data subject. Recital 58 states that the principle of transparency is of particular relevance in situations where the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him are

6 *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*. https://ec.europa.eu/newsroom/article29/items/612053/en

being collected, such as in the case of online advertising"[7]. This is particularly important in the case of telemedicine, as health data are involved, and the patient is not closely monitored by a doctor. The consequences of a mistake may even be lethal, and this is one of the reasons that led the European Commission to classify medical devices as "high risk systems".

Data controllers, which may be, for example, the hospital or the producer of the telemedicine device, must provide information about the processing and how ADM and profiling might affect data subjects. In Convention 108+, Article 77 provides that "Data subjects should be entitled to know the reasoning underlying the processing of data, including the consequences of such a reasoning, which led to any resulting conclusions, in particular in cases involving the use of algorithms for automated decision-making including profiling. For instance, in the case of credit scoring, they should be entitled to know the logic underpinning the processing of their data and resulting in a "yes" or "no" decision, and not simply information on the decision itself. Having an understanding of these elements contributes to the effective exercise of other essential safeguards such as the right to object and the right to complain to a competent authority"[8]. Data subjects, in addition, have the right to express their views on ADM and profiling, the right to have the decision affecting them made by a human being, and the right to challenge the decision. In the case of AI-based telemedicine, it may be extremely difficult to manage the remote health care process in such a way that the physician oversees each and every decision made by the system and at the same time ensure that only the physician makes the decision, as this may negate the benefit of using an automated decision. Even if the doctors managed to be constantly present, in the case of continuous learning they still will not be able to tell the patient how the system may behave with them. This will probably be possible in some cases, but in the future, if these devices become widespread and a high degree of integration of telemedicine into the health service on the ground is achieved, it will be essential to keep a close watch on the aspects just outlined. Another major problem of continuous learning systems is the difficult exercise of the right to challenge the system's decision, i.e. the lack of "contestability» of its outputs, defined as "lack of an obvious means to challenge them when they produce unexpected, damaging, unfair or discriminatory results» (Edwards & Veale, 2017). Not only the patient is unable to challenge the decision of the system, but so is a distant doctor, who cannot gather all the relevant elements that were employed by the system to reach its decision (e.g., the change in the daily medicine dosage). The proposed "contestability by design» (Almada, 2019) is thus inherently inapplicable to these models. In this scenario, it is possible to argue that, for the

7 *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.* https://ec.europa.eu/newsroom/article29/items/612053

8 *Ibid.* Art. 29.

sake of transparency and fairness, interpretable AI models should be used as a standard in telemedicine and black boxes should be employed only in cases in which the health care professional is able to closely oversee the output of the system and make a larger clinical assessment, based on additional elements other than the AI output. Also, continuous learning should be limited only to decisions which are not able to harm the patient in case of errors, and should be constantly monitored by a health care professional.

6. Informed Consent

When the legal basis that allows the processing of the patient's health data is consent, which is often the case for telemedicine devices, then GDPR requires it to be both explicit and informed, other than freely given, specific, and unambiguous. Other than the usual elements that should be communicated to the data subject according to the applicable law, additional information should be provided about how the virtual consultation is performed. This information includes rights under data protection regulations, the possibility of errors in the system, contact protocols during tele-consultations, prescribing policies, and coordination of care with other professionals (Membrado, 2021). Additional transparency requirements are found in the AI Act: article 13 lists the information that should be provided to the users, who also needs to be properly instructed regarding the AI system: High-risk AI systems shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to users. A detailed technical documentation is required by Article 11 and 18, which also add the requirement of keeping it up to date before the release of the system. The guidelines on ADM note that Data controllers seeking to rely on consent as a basis for profiling will need to demonstrate that data subjects understand exactly what they are consenting to, and remember that consent is not always an appropriate basis for processing. In all cases, data subjects should have enough relevant information about the intended use and consequences of the processing to ensure that any consent provided represents an informed choice. It might be argued that this is inherently not possible in the case of continuous learning, as even the doctor or the modelist will not be able to predict the consequences of using an unpredictable model. The information received by the patient needs to be concise, transparent, intelligible and in an easily accessible form, using clear and plain language, depending on the audience, adapted to the age, mental ability, and education level of the data subjects. In any case, it is only possible to use ADM and profiling with special categories of data, such as medical data, if there is explicit consent from the data subject or if it is permitted by law for substantial reasons of public interest, provided there are adequate safeguards in place. It is not enough to use public interest as a legal basis, it must also be considered substantial. It can be argued, for example, that a use aimed at combating Covid-19 falls within the "substantial public interest" grounds. Informed consent,

both from a legal and ethical point of view, becomes a central element of AI systems employed in telemedicine.

7. Vulnerable Groups

An open issue Telemedicine using intelligent systems raises more concerns when particularly vulnerable subjects are involved, such as oncological patients, patients with cognitive problems – for example, elderly people suffering from senile dementia or Alzheimer's disease-, children, neurodiverse patients (Shaw et al., 2022), or people who do not speak the language used by the doctor. First, a major issue is the ability to provide consent that is informed, free, unambiguous, and specific (Art. 7 GDPR). The doctor-patient relationship is itself an unbalanced one, where the parties are not on the same level, and where the patient is in a vulnerable situation; it may be particularly difficult to obtain consent that meets all the requirements of the law from a fragile individual, such as a cancer patient, already prostrated by the disease, might be.

If we add to this the right to obtain an explanation, it becomes clear that several problematic points may arise: in telemedicine, the doctor is far from the patient, and human contact is completely lacking. Explanations given remotely may be unclear or misunderstood, as the patient is unable to clearly see the signals of nonverbal communication.

Since these are AI systems, whose functioning, even in the case of explainable and interpretable AI, is often obscure even to experts, the risks of misunderstanding become significant and difficult to eliminate, unless a live consultation is also provided. When the system behavior is not predictable, it becomes even more difficult to explain the consequences of using the device to a vulnerable patient.

Also to be kept in mind is the digital divide, that is, the fact that not all patients have the same degree of digital literacy. This circumstance takes on significant weight in the case of telemedicine services provided in the public sphere, since there would be discrimination between users who are able to use the service and users who, for various reasons, are not. This risk is also underlined by the European Commission, which based its opinion, among other things, on the OECD report "Health at a Glance: Europe - 2018", according to which there is a risk of discrimination between users who are able to use the service and those who are not.

The Commission notes that there is a direct relationship between the level of education and the number of searches for health information on the web; in fact, similar disparities in the use of digital solutions for health promotion and disease prevention are also likely, and there is a risk that digital tools such as apps, wearable technology, and online forums will not benefit those who need them most, potentially widening health-related inequalities (Oliveira, 2020). The divide may even be exacerbated by continuous learning systems, as those who are better at using the telemedicine devices are more likely to get a more precise output. This risk should be evaluated by health care professionals when delivering tele-health services.

8. The Balance Between Privacy and Protection from Harm at Distance

As we discussed above, one of the major problems of continuous learning in telemedicine is that the model "evolves" while the patient is physically distant from the doctor (and from the IT support) and at the same time the system is usually designed to be less intrusive as possible. This leads to the necessity for a balance between constantly monitoring patients to ensure their safety and preserving their privacy, without making them feel uncomfortable with the technology. Therefore, four elements become relevant: technical measures, organizational measures, psychological factors, and legal requirements. From a technical point of view, a number of different techniques have been studied to solve some of the privacy issues discussed above, such as problems related to identity management, using blockchain, encryption, or federated learning under edge computing (Ahmad, 2021; Jain et al., 2022; Wang, 2021; Ma et al., 2020; Wang, 2022).

However, some of the problems cannot be solved only using technology: organizational measures play a crucial role in achieving the balance between the protection of privacy and the benefits of surveillance technology as a countermeasure against unexpected malfunction of the system.

In fact, as a first measure, the harm caused by malfunctions of the system can be mitigated by scheduling appropriate maintenance interventions delivered by IT experts and medical doctors, who can test the system, evaluate its performance, and assess the patient's health. These measures can be enacted keeping the burden on patients at the very minimum (e.g., combining the maintenance to the regular in-person appointments at the hospital). However, a second measure is equally important: training doctors and patients on the correct use of telemedicine technology is crucial both to preserve privacy and to mitigate the risk of malfunctioning and incorrect use. Once doctors are correctly trained, for example, they may be able to recognize peculiar and unique features of patients that could lead the self-learning system to generate errors.

From a psychological point of view, vulnerable patients may need additional support with: understanding the functioning of the system in order to be able to use it correctly and express a free informed consent; accepting the system in their life without feeling a disruption of everyday activities; learn how to express their concerns and discomfort (including physical pain) at a distance (Yakar, 2021).

A trained therapist, working together with doctors and IT experts, could be appointed to help patients in overcoming those issues. On the other hand, doctors should make sure that patients are able to understand their instructions and they should regularly check if their consent is truly informed. Privacy law is not an obstacle against the enacting the above-mentioned measures, as GDPR provides for appropriate means to protect patients' fundamental rights. As an additional organizational measure, hospitals should appoint a privacy expert to monitor the use of telemedicine devices and to guide all the stakeholders.

9. AI Auditing Measures as an Additional Safeguard

The academic field of algorithmic auditing within the broader AI auditing framework is becoming more and more popular in the recent years, especially in the domain of machine learning. AI auditing means incorporating Ethics, Human Rights, and Law into the whole AI development life cycle and in the post-market phase (LaBrie & Steinke, 2019; Mökander & Floridi, 2022; Mantelero & Esposito, 2021; Koshiyama et al., 2021; Mökander, 2022; Floridi, 2022), while at the same time checking its technical soundness (e.g., safety, security, performance, and correctness of pre-processing techniques). To this aim, many practical tools have been created, such as several Ethics Canvas (e.g., the Open AI Canvas, the Data Ethics Canvas, the AI Ethics Canvas (Kalra, 2020). This type of assessment and continuous monitoring is important to detect biases, technical and statistical errors, security flaws, and detrimental effects during the post-market phase. In fact, due to the close look into the whole processes and the compliance mechanism enacted since the early stages of the AI development (i.e., even before the data collection), it is possible to prevent many of the errors that could lead to privacy violation, errors in the system, security breaches, and discrimination. It is therefore recommended to implement AI auditing procedures every time continuous learning models are envisaged in clinical practice.

Conclusions

In this brief contribution we have seen how telemedicine carried out through continuous learning intelligent systems is a useful tool to ensure better health care to the patient, but that its diffusion may also bring new challenges to the jurist and to health care professionals. New legal problems, such as the regulation of systems that adapt to the patient or the protection of vulnerable subjects, and their ability to understand how the AI system works, in order to be able to express a free consent, will have to be addressed and dissected by the doctrine in the near future. Health care facilities intending to employ AI systems to deliver telemedicine services should train their employees and the patients to handle the system safely and securely, in order to avoid data breaches and an incorrect use of the devices. An efficient way to achieve this goal is to have dedicated teams of IT experts, doctors, and trained therapists. Although the European Union has tried to give a legal response to the development of AI techniques, there are still many unresolved issues. It is hoped, therefore, that the issue can be adequately explored before telemedicine through AI techniques becomes a widespread and common practice on the EU territory.

References

Ahmad, R. W. (2021). The role of blockchain technology in telehealth and telemedicine. *International Journal of Medical Informatics*, *148*, 104399. https://doi.org/10.1016/j.ijmedinf.2021.104399

Almada, M. (2019). Human intervention in automated decision-making: Toward the construction of contestable systems. In *Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law* (pp. 2–11). https://doi.org/10.2139/ssrn.3264189

Botrugno, C. (2014). Un diritto per la telemedicina: analisi di un complesso normativo in formazione. *Politica del Diritto*, *4*(45), 639–668. https://doi.org/10.1437/78949

Burrai, F., Gambella, M., & Scarpa, A. (2021). L'erogazione diprestazioni sanitarie in telemedicina. *Giornale di Clinica Nefrologica e Dialisi*, *33*, 3–6.

Campagna, M. (2020). Linee guida per la Telemedicina: considerazioni alla luce dell'emergenza Covid-19. *Corti Supreme e Salute*, *3*, 11–25.

Castagno, S., & Khalifa, M. (2020). Perceptions of artificial intelligence among healthcare staff: a qualitative survey study. *Frontiers in artificial intelligence*, *2*(5), 84–92. https://doi.org/10.3389/frai.2020.578983

Davis, E. (2016). AI Amusements: The Tragic Tale of Tay the Chatbot. *AI Matters*, *2*(4), 20–24. https://doi.org/10.1145/3008665.3008674

Edwards, L., & Veale, M. (2017). Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for. *Duke L. & Tech. Rev.*, *16*, 18–26.

Floridi, L. (2022). capAI-A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4064091

Gallese, Ch. (2022). Suggestions for a revision of the European smart robot liability regime. In *Proceedings of the 4th European Conference on the Impact of Artificial Intelligence and Robotics (ECIAIR 2022)*. https://doi.org/10.34190/eciair.4.1.851

Gioulekas, F. (2022). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. *Healthcare*, *10*, 327–333. https://doi.org/10.3390/healthcare10020327

Giunti, G. (2014). The Use of a Gamified Platform To Empower And Increase Patient Engagement in Diabetes Mellitus Adolescents. In *American Medical Informatics Association Annual Symposium*.

Jain, N., Gupta V., & Dass, P. (2022). Blockchain: A novel paradigm for secured data transmission in telemedicine. In *Wearable Telemedicine Technology for the Healthcare Industry* (pp. 33–52).

Kalra, A. (2020). *Artificial Intelligence Ethics Canvas: A Tool for Ethical and Socially Responsible AI*.

Koshiyama, A. S., Kazim, E., Treleaven, P. C., Rai, P., Szpruch, L., Pavey, G., Ahamat, G., Leutner, F., Goebel, R., Knight, A., Adams, J., Hitrova, C., Barnett, J., Nachev, P., Barber, D., Chamorro-Premuzic, T., Klemmer, K., Gregorovic, M., Khan, S. A., & Lomas, E. (2021). Towards Algorithm Auditing: A Survey on Managing Legal, Ethical and Technological Risks of AI, ML and Associated Algorithms. *Software Engineering eJournal*. https://doi.org/10.2139/ssrn.3778998

LaBrie, R., & Steinke, G. (2019). Towards a framework for ethical audits of AI algorithms. In *Twenty-fifth Americas Conference on Information Systems*.

Lakkaraju, H. (2019). Faithful and customizable explanations of black box models. In *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 131–138). https://doi.org/10.1145/3306618.3314229

Ma, M., Shuqin, F., & Feng, D. (2020). Multi-user certificateless public key encryption with conjunctive keyword search for cloud-based telemedicine. *Journal of Information Security and Applications*, *55*, 102652. https://doi.org/10.1016/j.jisa.2020.102652

Mantelero, A., & Esposito, S. (2021). An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems. *Computer Law & Security Review*, *41*, 105561. https://doi.org/10.1016/j.clsr.2021.105561

Marchant, G., & Lindor, R. (2012). The coming collision between autonomous vehicles and the liability system. *Santa Clara Law Review*, *52*, 1321–1340.

Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and information technology*, *6*, 175–183. https://doi.org/10.1007/s10676-004-3422-1

Membrado, C. G. (2021). Telemedicina, ética y derecho en tiempos de COVID-19. Una mirada hacia el futuro. *Revista Clinica Espanola*, *221*, 408–410. https://doi.org/10.1016/j.rce.2021.03.002

Mi, F. (2020). Generalized Class Incremental Learning. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops* (pp. 240–241).

Mökander, J. (2022). Conformity assessments and post-market monitoring: a guide to the role of auditing in the proposed European AI regulation. *Minds and Machines*, *32*, 241–268. https://doi.org/10.1007/s11023-021-09577-4

Mökander, J., & Floridi, L. (2022). Operationalising AI governance through ethics-based auditing: an industry case study. *AI and Ethics*, *6*, 1–18. https://doi.org/10.1007/s43681-022-00171-7

Oliveira, T. (2020). Bringing health care to the patient: An overview of the use of telemedicine in OECD countries. *OECD, Directorate for Employment, Labour and Social Affairs, Health Committee*.

Pacis, D., Mitch, M., Edwin, D. C., Subido, Jr., & Bugtai, N. (2018). Trends in telemedicine utilizing artificial intelligence. In *AIP conference proceedings*. AIP Publishing LLC.

Parisi, G. (2019). Continual lifelong learning with neural networks: A review, *Neural Networks*, *113*, 54–71. https://doi.org/10.1016/j.neunet.2019.01.012

Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology*, *4*, 100005. https://doi.org/10.1016/j.jrt.2020.100005

Schatten, M., & Protrka, R. (2021). Conceptual Architecture of a Cognitive Agent for Telemedicine based on Gamification. In *Central European Conference on Information and Intelligent Systems* (pp. 3–10).

Scheetz, J. (2021). A survey of clinicians on the use of artificial intelligence in ophthalmology, dermatology, radiology and radiation oncology. *Scientific reports*, *11.1*, 1–10.

Shaw, S., Davis, L-J., & Doherty, M. (2022). *Considering autistic patients in the era of telemedicine: the need for an adaptable, equitable, and compassionate approach, BJGP open 6.1*.

Strehle, E. M., & Shabde, N. (2006). One hundred years of telemedicine: does this new technology have a place in paediatrics? *Archives of disease in childhood*, *91.12*, 956–959. https://doi.org/10.1136/adc.2006.099622

Tigard, D. (2020). There is no techno-responsibility gap. *Philosophy & Technology*, 1–19.

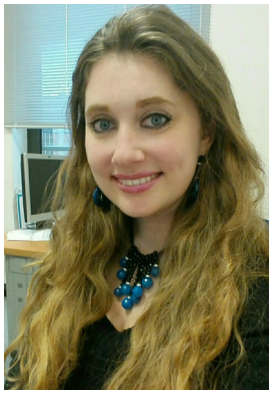
Wang, R. (2022). Privacy-Preserving Federated Learning for Internet of Medical Things under Edge Computing. *IEEE Journal of Biomedical and Health Informatics*.

Wang, W. (2021). A privacy protection scheme for telemedicine diagnosis based on double blockchain. *Journal of Information Security and Applications*, *61*, 102845. https://doi.org/10.1016/j.jisa.2021.102845

Yakar, D. (2021). Do People Favor Artificial Intelligence Over Physicians? A Survey Among the General Population and Their View on Artificial Intelligence in Medicine. *Value in Health*, *3*, 12–23. https://doi.org/10.1016/j.jval.2021.09.004

Ye, J. (2020). The role of health technology and informatics in a global public health emergency: practices and implications from the COVID-19 pandemic. *JMIR medical informatics*, *8.7*, e19866. https://doi.org/10.2196/19866

Author information



Chiara Gallese Nobile – PhD, Researcher (postdoc) of research data management, Eindhoven University of Technology (Eindhoven, Netherlands), Researcher (postdoc) of the Department of Mathematics and Geosciences, University of Trieste (Trieste, Italy).
Address: P/O 513 5600 MB Eindhoven, the Netherlands
E-mail: cgallese@liuc.it
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 interests

The author is an international editor of the Journal; the article has been reviewed on general terms.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – May 4, 2023
Date of approval – May 20, 2023
Date of acceptance – June 16, 2023
Date of online placement – June 20, 2023

Научная статья
УДК 347.1:654:004.8
EDN: https://elibrary.ru/vskcfb
DOI: https://doi.org/10.21202/jdtl.2023.13

Правовые аспекты использования искусственного интеллекта в телемедицине

Кьяра Галлезе-Нобиле

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

Ключевые слова

Законодательство,
защита данных,
искусственный интеллект,
персональные данные,
право,
регулирование,
телемедицина,
цифровое неравенство,
цифровые технологии,
частная жизнь

Аннотация

Цель: стремительное распространение телемедицины в клинической практике и возрастающая роль искусственного интеллекта ставят перед юристами множество проблем относительно охраны неприкосновенности частной жизни. Повышенная сензитивность данных в этой области заставляет уделить особое внимание правовым аспектам таких систем. В статье исследуются правовые последствия использования искусственного интеллекта в телемедицине, в частности, систем непрерывного обучения и автоматизированного принятия решений; фактически оказание персонализированных медицинских услуг через системы непрерывного обучения может представлять дополнительный риск. Особого внимания заслуживают уязвимые группы населения – дети, пожилые люди и тяжелобольные пациенты – как по причине цифрового неравенства, так и из-за сложностей с выражением своего согласия.

Методы: сравнительно-правовые и формально-правовые методы исследования позволили проанализировать текущее состояние регулирования искусственного интеллекта и выявить его соотношение с нормами регулирования телемедицины, Общим регламентом ЕС по защите персональных данных и другими нормами.

Результаты: изучены правовые последствия использования искусственного интеллекта в телемедицине, в частности, систем непрерывного обучения и автоматизированного принятия решений; автор приходит к выводу, что оказание персонализированных медицинских услуг через системы непрерывного обучения представляет дополнительные риски, и предлагает пути их минимизации. Автор также уделяет особое внимание вопросам информированного согласия уязвимых групп населения (детей, пожилых, тяжелобольных).

Научная новизна: изучены актуальные риски и проблемы, возникающие в сфере использования искусственного интеллекта в телемедицине, при этом особое внимание уделено системам непрерывного обучения.

Практическая значимость: полученные результаты восполняют недостаток научных исследований по данной теме, могут быть использованы в законодательном процессе в сфере использования искусственного интеллекта в телемедицине, а также в качестве основы для будущих исследований в данной области.

Для цитирования

Галлезе-Нобиле, К. (2023). Правовые аспекты использования искусственного интеллекта в телемедицине. *Journal of Digital Technologies and Law*, *1*(2), 314–336. https://doi.org/10.21202/jdtl.2023.13

Список литературы

Ahmad, R. W. (2021). The role of blockchain technology in telehealth and telemedicine. *International Journal of Medical Informatics*, *148*, 104399. https://doi.org/10.1016/j.ijmedinf.2021.104399

Almada, M. (2019). Human intervention in automated decision-making: Toward the construction of contestable systems. In *Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law* (pp. 2–11). https://doi.org/10.2139/ssrn.3264189

Botrugno, C. (2014). Un diritto per la telemedicina: analisi di un complesso normativo in formazione. *Politica del Diritto*, *4*(45), 639–668. https://doi.org/10.1437/78949

Burrai, F., Gambella, M., & Scarpa, A. (2021). L'erogazione diprestazioni sanitarie in telemedicina. *Giornale di Clinica Nefrologica e Dialisi*, *33*, 3–6.

Campagna, M. (2020). Linee guida per la Telemedicina: considerazioni alla luce dell'emergenza Covid-19. *Corti Supreme e Salute*, *3*, 11–25.

Castagno, S., & Khalifa, M. (2020). Perceptions of artificial intelligence among healthcare staff: a qualitative survey study. *Frontiers in artificial intelligence*, *2*(5), 84–92. https://doi.org/10.3389/frai.2020.578983

Davis, E. (2016). AI Amusements: The Tragic Tale of Tay the Chatbot. *AI Matters*, *2*(4), 20–24. https://doi.org/10.1145/3008665.3008674

Edwards, L., & Veale, M. (2017). Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for. *Duke L. & Tech. Rev.*, *16*, 18–26.

Floridi, L. (2022). capAI-A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4064091

Gallese, Ch. (2022). Suggestions for a revision of the European smart robot liability regime. In *Proceedings of the 4th European Conference on the Impact of Artificial Intelligence and Robotics (ECIAIR 2022)*. https://doi.org/10.34190/eciair.4.1.851

Gioulekas, F. (2022). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. *Healthcare*, *10*, 327–333. https://doi.org/10.3390/healthcare10020327

Giunti, G. (2014). The Use of a Gamified Platform To Empower And Increase Patient Engagement in Diabetes Mellitus Adolescents. In *American Medical Informatics Association Annual Symposium*.

Jain, N., Gupta V., & Dass, P. (2022). Blockchain: A novel paradigm for secured data transmission in telemedicine. In *Wearable Telemedicine Technology for the Healthcare Industry* (pp. 33–52).

Kalra, A. (2020). *Artificial Intelligence Ethics Canvas: A Tool for Ethical and Socially Responsible AI*.

Koshiyama, A. S., Kazim, E., Treleaven, P. C., Rai, P., Szpruch, L., Pavey, G., Ahamat, G., Leutner, F., Goebel, R., Knight, A., Adams, J., Hitrova, C., Barnett, J., Nachev, P., Barber, D., Chamorro-Premuzic, T., Klemmer, K., Gregorovic, M., Khan, S. A., & Lomas, E. (2021). Towards Algorithm Auditing: A Survey on Managing Legal, Ethical and Technological Risks of AI, ML and Associated Algorithms. *Software Engineering eJournal*. https://doi.org/10.2139/ssrn.3778998

LaBrie, R., & Steinke, G. (2019). Towards a framework for ethical audits of AI algorithms. In *Twenty-fifth Americas Conference on Information Systems*.

Lakkaraju, H. (2019). Faithful and customizable explanations of black box models. In *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 131–138). https://doi.org/10.1145/3306618.3314229

Ma, M., Shuqin, F., & Feng, D. (2020). Multi-user certificateless public key encryption with conjunctive keyword search for cloud-based telemedicine. *Journal of Information Security and Applications*, *55*, 102652. https://doi.org/10.1016/j.jisa.2020.102652

Mantelero, A., & Esposito, S. (2021). An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems. *Computer Law & Security Review*, *41*, 105561. https://doi.org/10.1016/j.clsr.2021.105561

Marchant, G., & Lindor, R. (2012). The coming collision between autonomous vehicles and the liability system. *Santa Clara Law Review*, *52*, 1321–1340.

Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and information technology*, *6*, 175–183. https://doi.org/10.1007/s10676-004-3422-1

Membrado, C. G. (2021). Telemedicina, ética y derecho en tiempos de COVID-19. Una mirada hacia el futuro. *Revista Clinica Espanola*, *221*, 408–410. https://doi.org/10.1016/j.rce.2021.03.002

Mi, F. (2020). Generalized Class Incremental Learning. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops* (pp. 240–241).

Mökander, J. (2022). Conformity assessments and post-market monitoring: a guide to the role of auditing in the proposed European AI regulation. *Minds and Machines*, *32*, 241–268. https://doi.org/10.1007/s11023-021-09577-4

Mökander, J., & Floridi, L. (2022). Operationalising AI governance through ethics-based auditing: an industry case study. *AI and Ethics*, *6*, 1–18. https://doi.org/10.1007/s43681-022-00171-7

Oliveira, T. (2020). Bringing health care to the patient: An overview of the use of telemedicine in OECD countries. *OECD, Directorate for Employment, Labour and Social Affairs, Health Committee*.

Pacis, D., Mitch, M., Edwin, D. C., Subido, Jr., & Bugtai, N. (2018). Trends in telemedicine utilizing artificial intelligence. In *AIP conference proceedings*. AIP Publishing LLC.

Parisi, G. (2019). Continual lifelong learning with neural networks: A review, *Neural Networks*, *113*, 54–71. https://doi.org/10.1016/j.neunet.2019.01.012

Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology*, *4*, 100005. https://doi.org/10.1016/j.jrt.2020.100005

Schatten, M., & Protrka, R. (2021). Conceptual Architecture of a Cognitive Agent for Telemedicine based on Gamification. In *Central European Conference on Information and Intelligent Systems* (pp. 3–10).

Scheetz, J. (2021). A survey of clinicians on the use of artificial intelligence in ophthalmology, dermatology, radiology and radiation oncology. *Scientific reports*, *11.1*, 1–10.

Shaw, S., Davis, L-J., & Doherty, M. (2022). *Considering autistic patients in the era of telemedicine: the need for an adaptable, equitable, and compassionate approach, BJGP open 6.1*.

Strehle, E. M., & Shabde, N. (2006). One hundred years of telemedicine: does this new technology have a place in paediatrics? *Archives of disease in childhood*, *91.12*, 956–959. https://doi.org/10.1136/adc.2006.099622

Tigard, D. (2020). There is no techno-responsibility gap. *Philosophy & Technology*, 1–19.

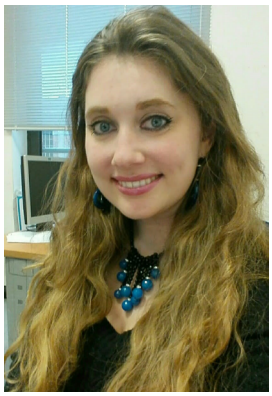
Wang, R. (2022). Privacy-Preserving Federated Learning for Internet of Medical Things under Edge Computing. *IEEE Journal of Biomedical and Health Informatics*.

Wang, W. (2021). A privacy protection scheme for telemedicine diagnosis based on double blockchain. *Journal of Information Security and Applications*, *61*, 102845. https://doi.org/10.1016/j.jisa.2021.102845

Yakar, D. (2021). Do People Favor Artificial Intelligence Over Physicians? A Survey Among the General Population and Their View on Artificial Intelligence in Medicine. *Value in Health*, *3*, 12–23. https://doi.org/10.1016/j.jval.2021.09.004

Ye, J. (2020). The role of health technology and informatics in a global public health emergency: practices and implications from the COVID-19 pandemic. *JMIR medical informatics*, *8.7*, e19866. https://doi.org/10.2196/19866

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
E-mail: cgallese@liuc.it
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 является международным редактором журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.27.91 / Гражданское право отдельных стран
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 4 мая 2023 г.
Дата одобрения после рецензирования – 20 мая 2023 г.
Дата принятия к опубликованию – 16 июня 2023 г.
Дата онлайн-размещения – 20 июня 2023 г.