

Artificial intelligence, privacy, and data protection in healthcare

Sofia B. Nunes¹, Rui Nunes¹

1. Faculdade de Medicina da Universidade do Porto, Porto, Portugal.

Abstract

The digital transition, particularly with regard to artificial intelligence, is shaping relationships among individuals and communities across a wide range of fields. This article aims to address, in a structured and systematic manner, cybersecurity as it relates to the preservation of civilizational values, such as privacy and the protection of personal health data, in the context of the digital transformation of contemporary societies. The article focuses primarily on the hypothesis that clear strategies for protecting health data are needed, given their particularly sensitive nature, including their access, storage, and sharing through modern digital systems. The authors suggest implementing creative measures that employ AI to assess privacy impacts during the design, development, acquisition, and implementation of digital systems. Requiring privacy impact studies or assessments would be an excellent tool for preventing disruptive cyber phenomena.

Keywords: Bioethics. Computer security. Artificial intelligence. Privacy. Health.

Resumo

Inteligência artificial, privacidade e proteção de dados na saúde

A transição digital, especialmente no que tange a inteligência artificial, molda as relações entre pessoas e comunidades nos mais diferentes domínios de atividade. Este artigo aborda de modo estruturado e sistemático, a cibersegurança no que diz respeito à preservação de valores civilizatórios, tais como privacidade, ou proteção de dados pessoais na saúde, diante da transformação digital das sociedades contemporâneas. O artigo trabalha centralmente a hipótese da necessidade de estratégias claras de proteção de dados de saúde, dada sua especial sensibilidade, incluindo acesso, armazenamento e partilha por meio dos modernos sistemas digitais. Os autores sugerem a implementação de medidas criativas, que recorram a IA, para avaliar o impacto na privacidade quando do desenho, do desenvolvimento, da aquisição e da implementação de sistemas digitais. A exigência de estudos ou pareceres de impacto na privacidade seria excelente ferramenta de prevenção de fenômenos cibernéticos disruptivos.

Palavras-chave: Bioética. Segurança computacional. Inteligência artificial. Privacidade. Saúde.

Resumen

Inteligencia artificial, privacidad y protección de datos en salud

La transición digital, especialmente en lo que respecta a la inteligencia artificial, configura las relaciones entre personas y comunidades en los más diversos ámbitos de actividad. Este artículo pretende abordar de manera estructurada y sistemática, la ciberseguridad en lo relativo a la preservación de valores civilizatorios, como la privacidad o la protección de los datos personales de salud, ante la transformación digital de las sociedades contemporáneas. El artículo se centra en la hipótesis de la necesidad de estrategias claras para la protección de los datos de salud, dada su especial sensibilidad, incluido su acceso, almacenamiento e intercambio mediante los modernos sistemas digitales. Los autores sugieren la implementación de medidas creativas que recurran a la IA para evaluar el impacto sobre la privacidad durante el diseño, desarrollo, adquisición e implementación de sistemas digitales. La exigencia de estudios o dictámenes de impacto sobre la privacidad constituiría una excelente herramienta para prevenir fenómenos cibernéticos disruptivos.

Palabras clave: Bioética. Seguridad computacional. Inteligencia artificial. Privacidad. Salud.

The authors declare no conflict of interest.

The advent of the Fourth Industrial Revolution—essentially a result of globalization and the digital age—has profoundly altered the model of economic and social development of civilized societies (economy 4.0). The current phase of technological development is characterized by the incorporation into society and the economy—namely in industrial production—of a wide range of information and communication technologies, such as artificial intelligence (AI), the internet (internet of things), and robotics, among others. Virtually all productive systems are affected, including the health system, with a high impact on the productivity and employment (quality and quantity) of new digitally-based global-scale business models. Historically, economic, social, and industrial evolution has been associated with different technological evolutions—Industry 1.0 and steam and coal; Industry 2.0 and assembly lines based on electricity; Industry 3.0 and automation; and Industry 4.0 and the internet and digital economy—which have implied a rebalancing of social development and political relations between peoples, States, and nations¹.

The rise and development of artificial intelligence, or even the generalization of the internet, have come to pose the problem into new terms. It is possible to even speak of economy 5.0, as we are now entering a new phase in which it is important to optimize the digital revolution, but always in the service of people, society, the economy, health, and the promotion of a sustainable environment², and, simultaneously, to develop regulatory and supervisory systems that enable the full exercise of inalienable rights of citizens, such as the right to individual privacy, including in the health care sector.

This is a highly current and relevant issue, given not only the uncontrolled growth of this technology but also the lack of transnational regulation for its application and use, which should comply with universal ethical principles, such as individual autonomy or justice and equity in access. Although multiple countries have advanced in laws and guidelines on artificial intelligence, there is still no transnational regulatory framework that guarantees global convergence and applicability, which keeps the issue open and justifies the investigation proposed here.

This article aims to adopt a structured and systematic approach to cybersecurity concerning the preservation of civilizational values, such as privacy, or the protection of personal data, given the digital transformation of contemporary societies. We address the hypothesis of the need for clear strategies for protection of health data—including access, storage, and sharing—considering their special sensitivity. It is also important to verify if physicians and other health care professionals have acquired adequate literacy in AI and digital health to face demands and challenges. This study is based on a theoretical review to conduct a documentary analysis using as selection and discussion criteria for the analyzed documents their scientific relevance and their impact on national and international public policies.

Global digital society

McLuhan and Powers argued, a few decades ago, that the centripetal movement induced by cultural globalization was rapidly transforming the planet into a true “global village”³. It is understood that this evolution was strongly driven by new information and communication technologies (ICT), which have become an integral part of sociocommunity life, especially for the new generations. This technological determinism, partly dictated by the enormous investment of civilized societies in digital literacy, resorts to the dematerialization of information systems as an intervention paradigm. The internet, email, social networks, or virtual databases such as the cloud have provided obvious benefits to humanity, and in the most diverse domains.

In health care, the digital revolution has been intensely felt, both in the strategic and operational management of organizations (in hospitals and in primary health care) and in the dematerialization of the clinical process (electronic health record), of medical prescriptions (digital prescriptions), of the scheduling of medical appointments (online scheduling of consultations and exams), or, also, in e-health, a new way for patients to interact with the health care system through telemedicine⁴.

In Brazil and Portugal (and in the European Union), the collection, storage, and transmission of personal data (image, signal, video) for review through information technologies (email, internet) have specific ethical and legal implications, regulated, respectively, by the General Data Protection Law⁵ and the General Data Protection Regulation⁶.

Regarding the most varied services—from online shopping, mobility and transport (like Uber) to games and betting, including, obviously, product marketing—digital platforms have revolutionized the way business is conducted on a global scale. This revolution also includes social communication, a sector in which not only traditional media (radio, television, newspapers, magazines) are gradually being replaced with new media (social networks, digital newspapers, websites, mobile apps, virtual worlds, multimedia, computer games, and interactive applications), but there is also an important paradigm shift.

This change translates into different cultural practices, more community-based, in which the instant apprehension of information, often without adequate critical appreciation, can originate concentric circles of information and, consequently, of opinion formation, which distort reality and form eventually distorted currents of thought (of which the uncontrolled growth of fake news, disinformation, is a good example). In medicine, this phenomenon can be especially complex due to its impact on patient health, such as the discourse against vaccination.

In Europe, the enormous importance of the digital transformation led the European Commission to present the innovative “Digital Agenda”⁷, one of the structural pillars of the Europe 2030 strategy, intrinsically associated with the growth objectives of the European Union. The central idea of the agenda is to exploit the dynamic use of information and communication technologies to foster innovation and economic progress in the European Union, with the aim of creating a Digital Single Market in Europe. Creating high-quality digital services, whether for work, leisure, or business, without artificial barriers and with high levels of protection, is the goal of this market.

In other words, this evolution is aimed at: improving consumer and business access (geoblocking, e-commerce, and distribution) to technologies; developing advanced digital networks and innovative services (telecommunications market, media services, IT security); fostering the digital economy (data economy, inclusive digital society, interoperability and standardization, digitalization of the European industry); and guaranteeing digital rights and principles (in compliance with the European Declaration on Digital Rights and Principles).

Brazil also has an ambitious digital transformation agenda on the way to the digital age, which is oriented toward the following goals⁸: improving connectivity; increasing trust in technologies; triggering digital innovation; promoting the digital transformation of the economy; updating the regulatory framework to protect health data and information security; and building a whole-of-government approach. To this end, a working group was established for the management of the Brazilian Artificial Intelligence Plan⁹, which denotes the current concern in the matter.

As a result of the unstoppable evolution of technology, there arise unavoidable ethical issues that require reflection and regulation in the form of national and international legislation. Such legislation must consider human rights and environmental sustainability so that the rights of future generations are not mortgaged, and so that the right to health is enjoyed by all in conditions of equity.

The digital transition decisively informs the relations between persons and communities in their most different domains. Virtually, our way of life is being restructured by this revolution, and it is necessary to create conditions to perceive such a change and to establish planetary critical awareness about the deviations that may occur, amplified by the absence of formal institutions on a global scale capable of regulating several of these activities.

The existence of big data, that is, an enormous quantity of data in different media and captured in very diverse ways, has revolutionized the way in which individual rights, considered civilizational aspirations, are perceived and protected in contemporary societies. Our personal data are in

fact at the mercy of digital systems and artificial intelligence, which makes it necessary to impose the bioethical principles of autonomy, individual liberty, justice, and equity.

Personal data protection

According to Tene and Polonetsky¹⁰, we live in an era of big data. Data have become the raw material of production, a new source of immense economic and social value. Advances in data mining and data analysis and the massive increase in computational power and data storage capacity have expanded the amount of information available to businesses, governments, and individuals. Furthermore, the growing number of people, devices, and sensors connected by digital networks has revolutionized the capacity to generate, communicate, share, and access data.

Data create enormous value for the global economy, driving innovation, productivity, efficiency, and growth. At the same time, as noted by Omer Tene and Jules Polonetsky¹⁰, the “data deluge” is followed by privacy concerns that could cause a regulatory backlash, dampening the data economy and stifling innovation.

Therefore, the perception is that a digital global society evokes concerns at different levels, especially regarding cybersecurity and the control and regulation of access to personal data, including metadata, that is, data that provide data about other data. These are essential for communication and interaction between different artificial intelligence systems, and are useful for describing information of any nature, whether medical, literary, or artistic.

This concept must be distinguished from data lake (including big data), that is, very diverse collections of data from different sources, in a structured or unstructured way, which tend to grow exponentially with the development of digital systems. Metadata are essential in medical and life sciences research, and are already currently used because they provide detailed information on demographics, sample types, processing methods, among others. They are also systematically used in the creation of case report forms, a fundamental

instrument for the development of clinical trials for new human medicines.

In this context, the regulatory framework must progressively implement the concept of FAIR data, an acronym for findable, accessible, interoperable and reusable. This concept is based on the principle that data and metadata are actionable by digital systems, since, due to the volume, complexity, and speed of creation of data of these systems, they are progressively relied upon to process data. The first step is to ensure the location of data and metadata, an essential component of data FAIRification, which must be accessible to researchers and computational systems, as well as the respective access authorizations obtained. This is an essential condition for trustworthy AI, as suggested by the European Commission¹¹.

Since the purpose of the FAIR strategy is to maximize data reuse, data and system interoperability is fundamental to optimize their analysis, storage, and processing. In medicine and research, FAIR data does not necessarily mean open data, given the sensitivity of health data. However, resorting to them provides numerous advantages, such as avoiding duplication of efforts, reusing data for new purposes, achieving the greatest possible impact with the investigation carried out, and contributing to scientific replicability and reproducibility. Thus, society's trust in new technologies grows¹¹.

Therefore, it is necessary to identify the main ethical problems regarding the collection, storage, analysis, transfer, and visualization of personal data¹². And, furthermore, if the “principle of purpose” in data collection is respected, so as to reassure society in this regard, requiring the data subject to perform a clear positive act indicating a free, specific, informed, and unequivocal manifestation of will that they consent to the processing of their data—through a written declaration, including in electronic format, or an oral declaration, for example. It is noted that the newly created “right to be forgotten” is a reflection of the widespread perception that information systems do not effectively guarantee citizenship rights. And, as noted by Correia, Rego, and Nunes¹³, this right must be progressively considered in the formulation of public policies.

In medicine, this practice of consent is especially relevant and should be known by physicians and other health care professionals in research involving human beings¹⁴. The annex presents an example of a specific consent document for personal data processing (distinct content from the informed consent form for participation in a study/research, although it may be contained in the same document).

The generalization of AI in medicine also raises a broader issue: the protection of individual privacy¹⁵, a concept that relates, but is not limited to data protection. The following should be considered health-related personal data: all data that reveal information about a person's physical or mental health, including information about analyses or examinations of a body part or bodily substance, or genetic data and biological samples. Personal data also includes any information about disease, disability, risk of disease, clinical history, clinical treatment, or physiological or biomedical condition.

It is noted that data protection includes genetic data, which, by their very nature and because they involve third parties (relatives of the index case), deserve special protection. Genetic data are personal data relating to the genetic, hereditary or acquired characteristics resulting from the analysis of a biological sample, namely the analysis of chromosomes, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA), or the analysis of another element that provides equivalent information¹⁶.

Therefore, it is essential to disseminate the perception, in society in general and in medicine in particular, that the collection and processing of biological products (including genetic information) must be clearly regulated and supervised, always within the scope of the creation of a biobank, that is, a bank of biological products.

Adopting privacy-enhancing technologies, such as encryption, metadata, or user interface, is essential today given new data extraction technologies, full-body scanners, or second-generation DNA sequencing. Whenever possible, individual health data should be anonymized or pseudonymized to protect personal privacy. The application of pseudonymization to personal data can reduce risks for data subjects and help data controllers comply with their protection obligations, especially the obligation to protect

individual privacy, a particularly relevant right that, in digital culture, tends to be neglected.

In fact, individual privacy is a fundamental right that protects one of the most significant values of a secular and pluralistic society, as it seeks to restrict unauthorized access by third parties—individuals, organizations, or the State itself—to the person in their multiple dimensions. Thus, reinterpreting Coolley's view, cited by Adams, on the existence of a *right to be let alone*¹⁷. This jurisprudential view from the late 19th century aims to affirm that the human person is guaranteed the right to anonymity, to be left alone, and to the reserve of individual intimacy, in any social, economic, political, or psychological context, and that legislation must clearly stipulate the legal framework in which privacy can be conditioned¹⁸.

Individual privacy is, on a formal level, a relatively new right, given that society, in its multiple forms of organization and historically subject to the most diverse cultural influences, has ancestrally subjected human beings to collective designs and to the satisfaction of basic community survival needs¹⁹. However, the roots of this right may lie in the demarcation, in Aristotle's view, between public and private, that is, the *polis* and the *oikos*.

From the perspective of Solove²⁰, privacy preservation requires that third parties refrain from certain activities that violate a person's spirit, mind, peace, physical space, or body. This right is consolidated in art. 12 of the Universal Declaration of Human Rights, which clearly states that *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*²¹. Progressively, the concept of privacy became associated with more robust forms of individual sovereignty, including the following dimensions:

- physical: the right to decide about one's own body;
- mental: the right to cognitive and moral freedom, without coercion and with free thought;
- decisional: the right to make decisions about oneself without external interference;

- informational: the right to keep personal information reserved (including personal data), requiring the obtention of consent for access, use, and storage of such information; professional secrecy (medical secrecy) stems from this dimension of privacy;
- patrimonial: the right to obtain, maintain, and manage assets and private property.

Hence the need to implement effective cybersecurity strategies, that is, to protect digital systems, programs, and networks against disruptive attacks and interference in the digital space. Cybersecurity aims to protect people, institutions, and societies from unauthorized access, alteration, or destruction of privileged information, with medicine and health being particularly sensitive areas due to the private nature of personal data.

Artificial intelligence and cybersecurity

The implementation of an effective cybersecurity program essentially requires active involvement of all partners, with the implementation of an adequate strategy and effective coordination of processes and technology. Therefore, it is necessary to know the potential of AI to prevent cyberattacks that resort to privacy-intrusive technologies, such as ubiquitous computing, internet of things, satellite data, blockchain, cryptocurrency, machine learning, automation, environmental technology, neurolinguistic technology, memetic technology (formal study of memes), grid technology, identity theft, data mining, smart cards, key loggers, and wireless networks.

Then, concrete physical and logical security measures must be implemented to prevent the harmful effects of cyberattacks or extreme phenomena, such as black swan events. This term, coined by Taleb²², refers to unpredictable, highly improbable phenomena, but with significant national or international impact, which are only recognized *a posteriori*. The COVID-19 pandemic is a recent example of a black swan event, and the use of AI in cybersecurity strategies can enable the prevention, or at least the mitigation, of the devastating impact of future pandemics, not only

on patient health but also on the control of radical changes in public behavior and supply chains.

The health care sector, given its strategic importance, is a priority target for cyberattacks, especially when amplified by AI, requiring the implementation of security tests to effectively protect patient personal data and privacy. Cybersecurity in health care is especially critical because hospitals and health centers regularly rely on digital technologies in their operations—such as telemedicine or electronic health records/electronic medical records—at the hardware, software level or via the cloud²³.

Over the past two decades, hospitals worldwide have become targets of cyberattacks, including terrorist cyberattacks²⁴, such as the attack on the Change Healthcare hospital in the United States in 2024, or on the Hospital Clinic, in Barcelona, in 2023. Therefore, developing preventive strategies to protect patient personal data is fundamental. From the perspective of Lv and Piccialli²⁵, it may even be necessary to resort to advanced mathematical systems, such as differential privacy technology, to protect individual identity and personal health data.

Furthermore, hacking, which is the act of identifying and exploiting the weaknesses of a system or network and subsequently accessing personal data or organizational information without authorization, is frequent. This type of action seeks financial gains (access to credit cards, for example), corporate espionage, or is carried out by a State (to obtain information, for example), and is made easier by the trend, ultimately for security, of video surveillance of public spaces or within organizations—including hospitals—of online monitoring of various activities.

This trend implies the implementation of complex encryption mechanisms, crucial for protecting online privacy and security, and a tool of major interest for protecting fundamental rights, such as the right to health protection. Encryption, especially when leveraged by artificial intelligence, ensures that individuals and organizations can securely and freely share information, without fear of its publicization by the State or criminal organizations. This includes sensitive information—such as gender identity, sexual orientation, positive status for some diseases, or reserved prognoses, such as in oncology—as well as

sensitive information in the private and public health care sectors (Unified Health System or National Health Service).

The approach to the need to implement global cybersecurity strategies, especially to address the issue of the possibility of protecting individual privacy in digital society and in expanded cyberspace (universal in the literal sense of the term), lacks an adequate conceptual framework.

This framework should intersect security and privacy in the ontological, epistemological, methodological, and bioethical dimensions, which is especially relevant considering the paradigm shift that is evident today²⁶. In fact, this AI-driven intersection represents a true paradigm shift, both from a scientific perspective²⁷ and an epistemological perspective²⁸. Thus, it is understood that the cybersecurity issue in global digital society will likely be one of the major challenges the international community will face in the coming decades. The interface between digital society, privacy, and global security can be analyzed from the perspective of positivism, and this analysis can be deepened through the appreciation of this paradigm in previously selected categorical dimensions.

In an ontological dimension, security is an objective necessity, on the level of personal well-being and also of the community, being of paramount importance in the global order and in the relations between different States. While privacy is a right formed by global consciousness, consensualized by mutual agreement between parties and ratified by methods acceptable to international institutions; it is the right opposite as a social value or a subjective interpretation of the concept of human dignity.

The epistemological dimension puts into perspective the lack of security, as observable reality and undeniable fact relating to the also objective truth of the need for protection. Hence the current reference to a global and collective social responsibility of different social actors for cybersecurity. In this dimension, the interference of the State and its agencies or multinational corporations, such as big-AI (for commercial, security, and social control reasons, among other), in private life is an undeniable reality.

While, in a methodological dimension, objective evidence of security failures leads to the necessity of implementing cybersecurity strategies. Given the hypothesis that only a strategy focused on the State organizational infrastructure level (or at the supranational governance level) can increase the level of digital security, the need to implement integrated cyber-governance strategies can be deduced. In fact, the repeated violation of individual privacy, a fact observable in cybersecurity failures, at different levels and in very diverse contexts, raises the need for broad national and international discussion on this issue. Eventually, it will be necessary to implement a true cyberpolicy at a transnational level, including the involvement of the United Nations or other international organizations in this regulation.

Bioethics ensuring security, especially in health data protection, is an essential condition for a physician-patient relationship in which trust continues to be a central element of the ethical and authentically human universe of clinical anamnesis. This assumption becomes an ethical imperative of major density when physicians are confronted with AI-driven digital systems, which physicians only partially control, given the lack of explanation about the technology. In fact, in medicine and health sciences, privacy is a bioethical value and a fundamental right in the physician-patient relationship, as it is an inherent right of the human person, resulting from their personal identity and the existence of a last refuge that must be safeguarded from any external interference. Privacy protection is also a pillar of the medical secrecy duty and of the very internal morality of medicine.

Some of the main security concerns in data protection are: confidentiality, in order to prevent unauthorized access, avoid sniffing (illegal data monitoring and traffic control), limit the sharing of access credentials and promote greater access control through encryption; and integrity, in order to prevent unauthorized modification of data, promote digital signatures, data validation, encoding and internal consistency methods, or avoid equipment failure, attacks or ransomware.

It is fundamental to anticipate this possibility of data protection insecurity by improving its

detection and preventing future occurrences. For very distinct reasons—including guaranteeing data authenticity (especially important in sectors such as health care, where much information with no scientific basis circulates on the internet and social media) and maintaining information integrity (so as to ensure storage without the possibility of unauthorized access)—it is important to define clear rules and coherent international policies. The digital single market policy in the European Union is a concrete example of the need to share data among different States, but also to implement coherent and structured security policies²⁹.

There are situations of threat to cognitive and structural security. There is also a non-negligible risk of total failure of critical infrastructures, as Myriam Dunn suggests: *The worst consequences of the risks created by information and communication technologies are manifested in the possible failure of the so-called critical infrastructures, which are systems and assets whose incapacitation or destruction would have a debilitating impact on national security and on the economic and social well-being of a state. Driven by a growing concern about the potential vulnerability of networked societies, along with an increasing number of disruptions in the cyber domain, several countries have taken measures to better understand the vulnerabilities and threats to their (information) infrastructures and have proposed measures for the protection of these assets*³⁰.

Naturally, this is a global issue, but also a focus of concern for each country. Thus, it is advised that each country propose and implement a national cybersecurity strategy, but always in coordination with other countries interested in implementing such policies. It is a fact that almost the entire population values cyberspace, implicitly or explicitly, given its ubiquity, scale, and intangibility³¹. Considering the level of digital literacy of the populations as consumers, including patients, this action is of paramount importance³², and includes the shared responsibility of different stakeholders, in order to create a complex and interconnected cybersecurity system.

In any case, given the lack of international institutions legitimized by the global order that effectively regulate these practices³³,

it seems important to continue promoting this reflection based on adequate theoretical and methodological assumptions. Thus, regardless of whether such regulation is carried out outside the traditional sovereignty of the State or rejects any exceptionality of cyberspace³⁴, well-founded solutions that realize the highest civilizational aspirations in this domain can be found—for example, and as we mentioned in another study³⁵, by framing trustworthy artificial intelligence within the broader scope of the United Nations Sustainable Development Goals.

Artificial intelligence has the capacity to revolutionize cybersecurity, as it enables: rapidly analyzing large amounts of data; detecting system anomalies and vulnerabilities (such as behavioral patterns); reacting in real-time, signaling suspicious behavior; automating repetitive processes, freeing up employees for other tasks; prioritizing risks and instantly detecting the possibility of malware and intrusions before they happen; and reducing human error.

Traditional cybersecurity relies on manual analysis, with signature-based detection, one of the basic security detection systems. It identifies malicious behaviors by searching a list of known indicators and has been reasonably effective against known threats. However, it does not respond to new or unknown threats.

Cybercriminal organizations have already invested heavily in AI to launch cyberattacks against specific organizations, and the health care sector is no exception. Despite that, the potential of AI in protecting digital systems is unlimited. Due to its speed, effectiveness, and efficiency, it substantially increases the productivity of security teams, especially in the face of new forms of cyberattack, such as malware or new scripting vectors.

The security of biometric data—data referring to specific human characteristics that enable the identification of an individual—is also considered of enormous relevance. Biometric identification systems and processes rely on the identification and comparison of physical or behavioral data, performed by complex digital systems, now enhanced by artificial intelligence. They include the use of fingerprints, facial recognition, genetic data, voice analysis, iris scanning, or palm scanning. On the behavioral

level, biometric identification resorts, for example, to the analysis of personal gait or facial expressions.

It is recurrently used to control attendance in the management of organizations, to monitor access—to promote cybersecurity and prevent unauthorized access to computers and other digital systems—and it is generally proof of personal identity. In Brazil, biometric identification is strongly regulated by the Brazilian Data Protection Law⁵ (LGPD); in Europe, by the General Data Protection Regulation⁶ and the AI Act¹⁵, given the potential for abuse and violation of fundamental rights. Other countries have produced regulatory initiatives, directives, and laws that address ethics, transparency, security, and responsibility in AI, albeit with different approaches: binding laws (South Korea), administrative directives (Japan), or specific legislation for damages and privacy (United States).

In medicine and life sciences, biometric identification is currently used regularly in scientific research and public health for epidemiological control. It is expected that, driven by AI, biometric identification may not only ensure personal data security but also promote more precise and personalized medical care³⁶.

Final considerations

The article addressed one of the essential dimensions of cybersecurity: the impact of AI on the protection of personal data and individual privacy in medicine and in society in general. Personal data cybersecurity may have multiple

value dimensions in the near future. That is, it can evolve from the positivist approach to the preservation of personal privacy (and therefore individual integrity) from the traditional perspective of relations between the individual and society (for example, States, health care system, large multinational pharmaceutical companies) to a distinct dynamics in which society promotes this type of interaction according to universal bioethical principles.

In conclusion, it is necessary to implement creative measures, which resort to AI, to assess the impact on privacy and data protection when designing, developing, acquiring, and implementing digital systems. Requiring privacy impact assessments or opinions would be an excellent means to prevent disruptive cybernetic phenomena that threaten the social perception of the benefits of AI. In any case, the digital transition and, in particular, artificial intelligence must always be under human supervision (human in the loop), and universally shared civilizational values must always be considered during its application.

Medicine and other health-related professions must be fully committed throughout the process of implementing AI systems in the field (physician in the loop), ensuring that the technology serves as a tool to support medical decision-making and does not violate fundamental rights of patients. This implies that medical training must implement educational strategies and literacy training in digital technologies so that physicians are fully included in and a core element of the digital transition.

References

1. Rawls J. The law of peoples. The idea of public reason revisited. Boston: Harvard University Press; 1999.
2. Mafi A, Holmes S. Artificial intelligence risks becoming an environmental disaster. *BMJ* [Internet]. 2025 [acesso 13 jan 2025];388. DOI: 10.1136/bmj.r505
3. McLuhan M, Powers B. The global village. New York: Oxford University Press; 1989.
4. Cornford T, Klecun-Drabowska E. Ethical perspectives in evaluation of telehealth. *Camb Q Healthc Ethics* [Internet]. 2001 [acesso 13 jan 2025];10(2):161-9. DOI: 10.1017/s0963180101002079
5. Brasil. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União* [Internet]. Brasília, 15 ago 2018 [acesso 21 jan 2025]. Disponível: <https://tinyurl.com/456hda6y>
6. Parlamento Europeu. Regulamento 2016/679. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito

- ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados. Jornal Oficial da União Europeia [Internet]. Bruxelas, p. 119-52, 4 maio 2016 [acesso 20 abril 2025]. Disponível: <https://tinyurl.com/23bx67r3>
7. Década digital da Europa [Internet]. Bruxelas: Comissão Europeia; 2024 [acesso 8 jan 2025]. Disponível: <https://tinyurl.com/5ccnpamn>
 8. Organisation for Economic Co-operation and Development. A caminho da era digital no Brasil [Internet]. Paris: OECD Publishing; 2020 [acesso 20 abr 2025]. DOI: 10.1787/45a84b29-pt
 9. Brasil. Resolução CITDIGITAL n° 2, de 8 de maio de 2025. Institui Grupo de Trabalho para a gestão do Plano Brasileiro de Inteligência Artificial. Diário Oficial da União [Internet]. Brasília, ed. 87, p. 2, 12 maio 2025 [acesso 7 nov 2025]. Seção 1. Disponível: <https://tinyurl.com/4ttxy9wd>
 10. Tene O, Polonetsky J. Privacy in the age of big data: a time for big decisions. Stanford Law Review Online [Internet]. 2012 [acesso 8 jan 2025];63:63-9. p. 63. Tradução livre. Disponível: <https://tinyurl.com/5n7wwpht>
 11. High-Level Expert Group on Artificial Intelligence. Ethics guidelines for trustworthy AI. Brussels: European Commission; 2019.
 12. Nicolaidou IL, Georgiades C. The GDPR: new horizons. In Synodinou TN, Jougoux P, Markou C, Prastitou T, editors. EU Internet Law – Regulation and Enforcement. Berlin: Springer; 2017. p. 3-18.
 13. Correia M, Rego G, Nunes R. Gender transition: is there a right to be forgotten? Health Care Anal [Internet]. 2021 [acesso 20 abril 2025];29:283-300. DOI: 10.1007/s10728-021-00433-1
 14. Lekadir K, Frangi AF, Porras AR, Glocker B, Cintas C, Langlotz CP *et al.* FUTURE-AI: international consensus guideline for trustworthy and deployable artificial intelligence in healthcare. BMJ [Internet]. 2025 [acesso 8 jan 2025];388:e081554. DOI: 10.1136/bmj-2024-081554
 15. European Union. Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. Brussels: European Union [Internet]; 2023 [acesso 20 abril 2025]. Disponível: <https://tinyurl.com/3pvh64h4>
 16. Nunes R. GeneÉtica. Coimbra: Almedina; 2013.
 17. Adams R. The right to be let alone. Fla Law Rev [Internet]. 1965 [acesso 3 mar 2025];17(4):597-608. Disponível: <https://tinyurl.com/y4dva5ck>
 18. Warren SD, Brandeis LD. The right to privacy. Harv Law Rev [Internet]. 1890 [acesso 3 mar 2025];4(5):193-220. Disponível: <https://tinyurl.com/dvww5kbx>
 19. Prosser W. Privacy. Calif Law Rev [Internet]. 1960 [acesso 3 mar 2025];48:383-423. DOI: 10.2307/3478805
 20. Solove DJ. A taxonomy of privacy. Univ PA Law Rev [Internet]. 2006 [acesso 3 mar 2025];154(3):477-560. Disponível: <https://bit.ly/4wodtnF>
 21. United Nations. Universal Declaration of Human Rights (1948) [Internet]. New York: United Nations; 2006 [acesso 12 ago 2026]. Disponível: <https://bit.ly/3SN7B9A>
 22. Taleb N. The black swan: the impact of the highly improbable. New York: Random House; 2008.
 23. Nunes R. Healthcare as a universal human right: sustainability in global health [Internet]. Milton Park: Routledge; 2022 [acesso 3 mar 2025]. Disponível: <https://bit.ly/4wLo9xq>
 24. Chen G, Jin G. Insights from evidence-based medicine method for building security systems against terrorist attacks in hospitals. J Multidiscip Healthc [Internet]. 2023 [acesso 3 mar 2025];16:4133-7. DOI: 10.2147/JMDH.S426166
 25. Lv Z, Piccialli F. The security of medical data on internet based on differential privacy technology. ACM Trans Internet Technol [Internet]. 2021 [acesso 3 mar 2025];21(3):1-18. DOI: 10.1145/3382769
 26. Banks M. The inter-paradigm debate. In: Light M, Groom AJR, editors. International relations: a handbook of current theory. London: Francis Pinter; 1985. p. 12-13.
 27. Kuhn T. The structure of scientific revolutions. Chicago: The University of Chicago Press; 1970.
 28. Popper K. Conjeturas e refutações. Coimbra: Almedina; 2003.

29. Digital single market policy. Europe 2020 Strategy [Internet]. Brussels: European Commission; 2018 [acesso 3 mar 2025]. Disponível: <https://bit.ly/4qZFeW>
30. Dunn M. A comparative analysis of cybersecurity initiatives worldwide. International Telecommunications Union. Genève: WSIS Thematic Meeting on Cybersecurity; 2005. p. 3. Tradução livre.
31. Choucri N, Madnick S, Ferwerda J. Institutions for cyber security. International responses and global imperatives. *Inf Technol Dev* [Internet]. 2014 [acesso 3 mar 2025];20(2):96-121. DOI: 10.1080/02681102.2013.836699
32. Miedema TE. Engaging consumers in cyber security. *Journal of Internet Law* [Internet]. 2018 [acesso 3 mar 2025];21(8):3-15.
33. Keohane R. International institutions: two approaches. *Int Stud Q* [Internet]. 1988 [acesso 3 mar 2025];32(4):379-96. DOI: 10.2307/2600589
34. Santos L. Regulação do ciberespaço: cesuristas e tradicionalistas. *Janus* [Internet]. 2015 [acesso 3 mar 2025];6(1):93-107. Disponível: <https://bit.ly/4qe10By>
35. Nunes R, Nunes S. Reliable Artificial Intelligence: The 18th Sustainable Development Goal. *Journal of Ethics and Legal Technologies* [Internet]. 2024 [acesso 3 mar 2025];6(2):1-19. DOI: 10.14658/pupj-JELT-2024-2-2
36. Nunes R, Nunes S. Inteligência artificial: uma ponte para o futuro da medicina. *Rev. bioét. (Impr.)* [Internet]. 2025 [acesso 30 out 2025];33(2):24-34. DOI: 10.1590/1983-803420254115PT

Sofia Nunes – PhD – asnunes@med.up.pt

 0000-0002-7182-9890

Rui Nunes – PhD – ruinunes@med.up.pt

 0000-0002-1377-9899

Correspondence

Sofia Nunes – Al. Prof. Hernâni Monteiro, 4200-319. Porto, Portugal.

Contribution of the authors

Sofia Nunes: conceptualization; investigation; methodology; resources; supervision; visualization; writing – original draft; writing – review & editing.

Rui Nunes: conceptualization; investigation; methodology; resources; supervision; visualization; writing – original draft; writing – review & editing.

Data availability: All data used or generated in this study are described and presented in full in the body of the article.

Editor in charge: Dilza Teresinha Ambrós Ribeiro

Received: 5.18.2025

Revised: 5.21.2026

Approved: 6.1.2026

Annex

DECLARATION OF CONSENT

(full name), holder of the National Identity Card/Citizen Card No. _____, declare that I freely and unequivocally grant _____
(organization name) consent for the processing of my personal data contained in _____
(study name), which will take place at _____
(name of the location where the study will be conducted), as well as for the subsequent processing of these data within the scope of this purpose.

I confirm that I have been informed that I have the right to request access to my personal data, to request its rectification, erasure, and portability, and that for any questions or complaints regarding personal data I must send an email to the Data Protection Officer of _____
(organization name), to the email address _____, as well as that I have the right to complain to the National Data Protection Authority/National Data Protection Commission.

I confirm that I have read the Privacy Policies of _____
(organization name), which can be found at (website).

(local), (date)

(Signature as per identification document)