REVIEW

ITALIAN JOURNAL OF PSYCHIATRY
2024;10:12-16; doi: 10.36180/2421-4469-2024-4

The risk perspective of AI in healthcare: GDPR and GELSI framework (Governance, Ethical, Legal and Social Implications) and the new European AI Act

Rocco de Filippis[1], Abdullah Al Foysal[2], Vincenzo Rocco[3], Riccardo Guglielmo[4], Barbara Sabatino[5,6] Andrea Pietropaoli[7], Francesco Boscarino[8], Antonio Vallese[9], Stefano Ferracuti[10]

[1] Institute of Psychopathology, Rome, Italy; [2] MS in Computer Engineering (AI), University of Genova, Genova, Italy; [3] Accountant, Rome, Italy; [4] University of Genova, Genova, Italy; [5] Mancini Law Offices, Rome, Italy; [6] Accountant Office Gulino-Rocco, Rome, Italy; [7] Lawyer, Advocate in the Supreme Court, Roma, Italy; [8] Degree in Economy; [9] Accountant, Rome, Italy; [10] Department of Human Neuroscience, Sapienza University, Rome, Italy

Summary

Objectives. Artificial intelligence (AI) is revolutionizing the way we live and interact with technology. However, its impact on privacy, transparency, the responsibilities of developers, users and beneficiaries, raises important ethical and legal questions. Already adopted in various sectors, such as commerce, marketing, communication and surveillance, AI, which is also powerfully appearing in the health sector, requires caution in balancing technological innovation with the protection of personal data in psychiatric patients.

Methods. To function and learn, AI systems require a huge amount of data. This collection often involves personal information, such as preferences, behaviors and biometrics data, as well as public data. People's privacy can be violated if data is used in an unauthorized way or if it is shared without the consent of the individuals involved. The use of AI-based algorithms can lead to the creation of detailed profiling of individuals. These profiling can be used to make decisions regarding accessibility to services. This can lead to discrimination based on unethical criteria, such as race, ethnic origin or political beliefs and health status. The pervasive use of AI can put essential elements of privacy at risk. The dissemination of sensitive information can compromise the privacy of individuals, making it easier to identify and expose private behaviors.

Results. *GDPR* and the forthcoming AI act represent the first examples of legislation at European level to regulate privacy protection in AI systems. European governments are adopting regulations that set limits on the use of personal data, protect individuals from algorithmic discrimination and ensure transparency in the use of AI systems Organizations should be held accountable for privacy failures and those involved should have the right to access, correct or delete their data.

Conclusions. Artificial intelligence has considerable potential, but requires caution in the management of personal data to protect the privacy of individuals. The collection and use of data should be balanced with respect for fundamental rights and freedoms. Privacy protection must be prioritized in the design and implementation of AI systems to ensure ethical and responsible use of this innovative technology.

Keywords: artificial intelligence, GDPR, GELSI, European AI Act

INTRODUCTION

Artificial intelligence (AI) is an increasingly present technology in our daily lives, and it has inevitable privacy implications, especially when considering psychiatric pathologies. All AI systems, before going into operation, adapt and build themselves

Correspondence
Rocco de Filippis
E-mail: roccodefilippis@istitutodipsicopatologia.it

How to cite this article:
de Filippis R, Al Foysal A, Rocco V, et al. The risk perspective of AI in healthcare: GDPR and GELSI framework (Governance, Ethical, Legal and Social Implications) and the new European AI Act. Italian Journal of Psychiatry 2024;10:12-16; https://doi.org/10.36180/2421-4469-2024-4

through a learning phase carried out by processes of collecting and analyzing a large amount of data, both personal and sensitive, in order to build an algorithm capable of providing results and suggestions relevant to the context of use.
The prospect, more or less in the short term, will be to be confronted with expert systems capable of significantly modifying the diagnostic and therapeutic paths in psychiatry, the decision-making modalities of the physician and, ultimately, also the physician-patient relationship. This raises several issues related to ethics, privacy and the responsibilities of the health professional towards the psychiatric patient.
Firstly, the collection and processing of large amounts of personal and sensitive data related to psychiatric vulnerability, such as familiarity, hospitalization or compulsory medical treatment can put people's privacy at risk. For instance, if personal information becomes accessible or falls into the wrong hands, it could be used for fraudulent or malicious purposes, or to exclude certain individuals from benefiting from certain services or to obtain them on more disadvantageous terms, e.g. profiling of patients for health insurance policies.
Secondly, AI can be used to monitor and profile individuals without their explicit consent. For instance, AI systems used for video surveillance can collect and analyze the facial characteristics of passers-by without their knowledge. This raises concerns about how the data is used and whether privacy rules are respected.
Furthermore, AI can lead to automated decisions that could have a significant impact on people's lives, and on the care services they receive. Patients may have difficulty understanding the reasons behind such decisions and may not be able to challenge or change them. This raises concerns about the transparency and fairness of AI-based decisions.
Furthermore, it is important to develop data anonymization and pseudonymization techniques to minimize the identifiability of individuals during data processing by AI systems. At the same time, organizations, including healthcare organizations, need to ensure transparency and inform people about how their data is used, giving them the opportunity to have control over the personal information they share.
Ultimately, AI offers great opportunities, but it is crucial to balance innovation with the need to protect people's privacy. Only through constant vigilance, appropriate regulations and increased user awareness can we ensure that AI and privacy can coexist safely and effectively.
The European Union [1] already has the GDPR, General Data Protection Regulation, which is a European regulation that came into force in May 2018, designed to protect and ensure the privacy of European citizens in all areas, including the digital sphere, by providing a number of basic rights for individuals regarding their privacy and protection of personal data. These rights include the right to be informed about how one's data is collected and used, the right to access one's personal data and request its modification or deletion, the right to data portability, and the right to withdraw consent to data processing.
In addition, the GDPR imposes a number of obligations on organizations that process personal data, including the need to collect only the data necessary for a specific purpose, inform individuals about their rights and how their data is processed, ensure data security and notify personal data breaches to the relevant authorities within 72 hours.
The extreme speed of dissemination of artificial intelligence, machine learning, automated decision-making tools together with the extreme speed of implementation and development of new technologies, new processes and tools, may generate the risk of being confronted with technologies not foreseen or foreseeable by existing regulation [2].
To address these concerns, it has long been clear to national and European legislators that it was necessary to establish regulations and policies that protect the privacy of collected data and its use through AI, either on the basis of existing data protection laws, such as the GDPR in Europe, which already provide a framework to guarantee privacy and ensure that data is used responsibly, or through the enactment of a more general and cross-sectoral regulation that can protect the design, implementation and use of AI systems.
On 21 April 2021, the European Commission [3] drafted the Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (AI Act), which the Council and the European Parliament approved, after more than two years of negotiations and at the end of a final 3-day negotiation, on 9 December 2023, thus issuing a Provisional Agreement of European Regulation on Artificial Intelligence, the so-called AI Act.
Under the European Regulation, software developed with one or more of the techniques and approaches specified in Annex I (which the Commission may amend over time by means of delegated acts) falls within the definition of an "AI system". Currently, these techniques include: machine-learning approaches; logic- and knowledge-based approaches; and statistical approaches, capable of generating, for a given set of human-defined objectives, outputs such as content, predictions, recommendations or decisions that influence the environments with which they interact.
The European AI Regulation is a legislative initiative that has the potential to promote the development and adoption by both public and private actors of secure and reliable AI across the EU single market. The main idea is to regulate AI on the basis of its ability to cause harm to society by following a 'risk-based' approach: the greater the risk, the stricter the rules. As the first legislative proposal of its kind in the world, it can set a global standard for regulating AI in other jurisdictions, as the General Data Protection Regulation has done, thereby promoting the European approach to regulating technology on the world stage.
In addition to public safety, the environment and democracy, great attention has also been paid to the issue of privacy and health protection. Precisely in the latter area, the impact of the large-scale use of artificial intelligence systems and devices could lead to substantial savings in resources and an accel-

eration towards personalized medicine and digital therapies. Or even more simply to the vast landscape of health apps that are able to increase patients' adherence to therapies and promote the adoption of healthy lifestyles [4].

SEARCH STRATEGY

In the European Regulation there is also a multilevel system of regulatory requirements depending on the inherent risk associated with the system and/or Artificial Intelligence practices used classified into: Prohibited AI Practices, High Risk AI Systems and Low Risk AI Systems.

In particular, the Regulations classify high-risk systems as all those that have the capacity to affect health. Therefore, any AI system in the medical-health field must necessarily be subject to the standards and controls envisaged for high-risk systems. In fact, high-risk AI systems include those technologies that present a significant risk of causing harm and whose use is therefore only permitted under specific safety controls. This part of the proposed IA Regulation adopts the approach taken in existing EU legislation on product safety and risk management in which IA systems related to essential public infrastructure, such as those that prioritize interventions or hospitalization, social security, medical devices, and diagnostic aids. High-risk systems include those AI systems whose use may have an impact on fundamental rights such as the right to health listed in Annex III of the Regulation [5].

The regulation imposes transparency and security obligations on such high-risk systems.

High-risk AI systems must be designed and developed to ensure that their operation is sufficiently transparent to enable users to interpret the output of the system and use it appropriately. The instructions and user manuals to be provided to the user must be clear and contain information regarding the identity of the supplier, the characteristics, capabilities and limitations of the AI system, and human supervision measures. The systems themselves must guarantee a high level of accuracy, robustness and security must be continuously ensured throughout the life cycle of the high-risk AI system. Serious incidents and malfunctions of the high-risk system must be reported immediately to the supervisory authorities of the Member State where the incident occurred.

In addition, the regulation incorporates [6] and imposes on the manufacturers of high-risk AIs a pre-marketing liability obligation, concretizing this obligation in numerous prior obligations such as:

1. complete and up-to-date technical documentation must be maintained (and compiled by the supplier prior to placing on the market or commissioning) to demonstrate compliance with the IA Regulation. The outputs of the high-risk IA system must be verifiable and traceable throughout its life cycle, including the automatic generation of logs (which must be kept by the providers, if under their control);
2. the system must be registered in a European database for high-risk AI systems before being placed on the market or put into service;
3. where an importer cannot be identified, providers established outside the EU will designate an authorised representative;
4. risk management: an appropriate risk management system must be established, implemented, documented and maintained as part of an overall quality management model. Risk management shall include a continuous iterative process throughout the life cycle of the system;
5. verification: any data set used to support training, validation and verification must be subject to appropriate data governance and management practices, be relevant, representative, error-free and complete, and have adequate statistical properties to support the use of the IA system;
6. human supervision: AI systems must be designed and developed in such a way as to enable effective human supervision, including in the AI training phase. This aspect of human supervision is also present in Article 22 of the GDPR concerning automated decision-making, in respect of which there is a right to obtain human intervention.

In addition to the above, providers are also required to:

a. establish, implement and maintain a post-market monitoring system (which is proportionate to the nature of the AI technologies and the risks of the high-risk AI system);
b. ensure that the system undergoes the relevant conformity verification procedure (before being placed on the market or put into service) and draw up an EU declaration of conformity;
c. take immediate corrective action with regard to high-risk IA systems found to be non-compliant (and inform the relevant national authority of such non-compliance and the action taken);
d. affix the CE marking to its high-risk IA systems to indicate compliance;
e. at the request of the competent national authority, demonstrate compliance of the high-risk IA system.

Importers, distributors and users of high-risk IA systems are also subject to stringent requirements. Some of the most important requirements for users of high-risk IA systems include: (i) using the systems in accordance with the instructions provided by the supplier; (ii) ensuring that all input data is relevant to its intended purpose; (iii) monitoring the operation of the system and informing the supplier/distributor of risks of serious incidents or malfunctions; and (iv) safeguarding the logs automatically generated by the high-risk IA system, if under their control.

Conformity Assessment, Notified Bodies/Notifying Authorities: the IA Regulation includes a conformity assessment procedure that must be followed for high-risk IA systems - with two different levels of assessment applied:

i. if the high-risk IA system is already governed by product safety regulations, a simplified conformity assessment applies, consisting essentially of an extension of the existing regime;
ii. for other high-risk AI systems (those listed in Annex III), the new compliance regime applies and the supplier is

required to self-assess compliance, except in the case of biometric remote identification systems, which will be subject to third-party compliance assessment.

The conformity assessment regime is supported by a network of notified bodies to be designated or established by Member States as independent third parties in the conformity process. Currently, and pending the final entry into force of the European Regulation on AI, manufacturers, operators and users of instruments, systems and processes based, even partially, on AI systems, must, however, deal with the requirements of the current GDPR, which already imposes limits and obligations that overlap with those in the new AI Act.

Article 25 of the GDPR imposes on providers the principle of 'data protection by design' (Art. 25(1) GDPR), in the implementation of artificial intelligence systems in the healthcare sector, appropriate technical and organizational measures must be taken to implement data protection principles (Art. 5 of the GDPR) and integrate into the processing the necessary safeguards to meet the requirements of the GDPR and protect the rights and freedoms of data subjects, similar to what has already been done with other national health information systems such as the TS System and the Electronic Health Record.

Art. 4 of the GDPR requires a correct identification of the roles of the data controller and the data processor, implementing a correct data governance, an overall vision of the ownership of the processing that takes into account that a national AI system in the health sphere could be accessed for different purposes by a multiplicity of subjects on the basis of different assumptions of lawfulness.

From another point of view, without prejudice to the need for processing in the sector under consideration to be legislatively attributed to the data controller, for the purpose of identifying in concrete terms the roles of the processing to be performed, it is indispensable to examine – on a substantive level – the competences attributed to the various subjects and, consequently, the activities concretely performed by them.

The GDPR sets out three cardinal principles that must govern the use of algorithms and AI tools in the performance of tasks of significant public interest:

1. the principle of knowability, according to which the data subject has the right to know about the existence of decision-making processes based on automated processing and, if so, to receive meaningful information about the logic used, so that he or she can understand it;
2. the principle of non-exclusivity of the algorithmic decision, according to which there must in any case exist in the decision-making process a human intervention capable of controlling, validating or refuting the automated decision (so-called human in the loop);
3. the principle of algorithmic non-discrimination, according to which it is advisable for the data controller to use reliable AI systems that reduce opacity, errors due to technological and/or human causes, periodically verifying their effectiveness also in the light of the rapid evolution of the technologies used, of the mathematical or statistical procedures appropriate for profiling, putting in place adequate technical and organizational measures. This is also to ensure that data inaccuracies are rectified and the risk of errors is minimized, given the potential discriminatory effects that the inaccurate processing of data on health status may have on individuals.

The GDPR then introduces the obligation for data controllers to carry out a prior impact assessment on processing that 'involves in particular the use of new technologies, having regard to the nature, subject-matter, context and purposes of the processing, may present a high risk to the rights and freedoms of natural persons' (Art. 35 GDPR), and to consult the Supervisory Authority where the technical and organizational measures identified to mitigate the impact of the processing on the rights and freedoms of data subjects are not deemed sufficient, or where the residual risk to the rights and freedoms of data subjects remains high (Art. 36 GDPR).

Art. 5 of the GDPR requires the data controller to ensure that the data are accurate and, where necessary, kept up to date, taking all reasonable steps to erase or rectify in a timely manner data that are incorrect in relation to the purposes for which they are processed.

DISCUSSION

The implementation and use of artificial intelligence tools in healthcare, whether for the execution of decision-making processes, diagnostic procedures, or the production of medical devices, provides, and in perspective will provide, enormous benefits in terms of a more effective and efficient management of scarce resources such as those related to the provision of healthcare services with the aim of supporting physicians in their daily practice and improving the therapeutic approach to patients. New smart technologies can reduce healthcare costs, avoiding numerous relapses and promoting personalized and home-based medicine. Scientific studies have already amply demonstrated how machine learning systems can improve patient prognosis and produce increasingly precise and accurate diagnoses.

The regulation agreement, which has been worked on for years, was approved on 9 December 2023 and lays the foundation for a more rapid deployment of artificial intelligence-based systems and applications within the entire healthcare system. The declared objective of the European Union, in fact, is also to incentivize all investments and innovations in the field of artificial intelligence, favoring the development of a market that is certainly complex, but which also has enormous potential, in the health sector and not only by overcoming the risks perceived by operators to make substantial investments in new technologies that might then turn out not to comply with the new enacted rules on AI.

When it comes to artificial intelligence algorithms, the main challenge is to succeed in promoting innovation and the adoption of new technological tools while fully respecting people's fundamental rights.

CONCLUSIONS

It is often repeated that artificial intelligence is revolutionizing the healthcare sector with the aim of supporting doctors in their daily practice and improving the therapeutic approach to patients. In addition to real-time data acquisition devices and medical robots that base their operation on machine learning, numerous medical devices also incorporate intelligent or metaverse-based software. New smart technologies can reduce healthcare costs, avoiding numerous relapses and promoting the personalized and home-based medicine that psychiatry so desperately needs. Scientific studies have already amply demonstrated how machine learning systems can improve patient prognosis and produce increasingly precise and accurate diagnoses.

The enactment of the European Regulation on AI is therefore an indispensable step in the development of AI systems in healthcare in order to protect all the rights that users and patients must have when using such automated systems (privacy, security, non-discrimination, human supervision) by overcoming and expanding the protections provided so far only by the GDPR on data privacy.

Conflict of interest statement

The authors declare no conflict of interest.

Funding

No funding institution had any role in the design, interpretation or publication of this study. The authors report no financial or other relationships relevant to the subject of this article.

Authors' contribution

R.d.F. conceived and designed the research, wrote the first draft of the manuscript and revised it with A.A.F., R.d.F. and V.R. supervised, B.S., A.P. and A.V. managed the literature search, extracted data relevant to the study and contributed to the interpretation of the data commetted by S.F. All authors contributed and approved the final manuscript.

References

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

2 Willke H. Smart governance: governing the global knowledge society. Campus Verlag 2007.

3 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 com2021/206

4 Tripathy AK, Carvalho R, Pawaskar K, et al. (2015, February). Mobile based healthcare management using artificial intelligence. In 2015 International Conference on Technologies for Sustainable Development (ICTSD) (pp. 1-6). IEEE.

5 Annex III-high-risk ai systems referred to in article 6(2) in 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 com2021/206.

6 Ethics guidelines for trustworthy AI. Report, Study. 8 aprile 2019.