Review Article

BIOMEDICAL Journal of Scientific & Technical Research

ISSN: 2574 -1241

DOI: 10.26717/BJSTR.2024.55.008761

Privacy in the Age of Artificial Intelligence

Fereniki Panagopoulou*

Assistant Professor, Panteion University, Greece

***Corresponding author:** Fereniki Panagopoulou, Assistant Professor, Panteion University, Greece

ARTICLE INFO

Received: March 19, 2024

Published: March 28, 2024

Citation: Fereniki Panagopoulou. Privacy in the Age of Artificial Intelligence. Biomed J Sci & Tech Res 55(5)-2024. BJSTR. MS.ID.008761.

Introduction

The extensive collection and general processing of our personal data that is necessary for the operation of artificial intelligence raises important concerns regarding the compatibility of technology with the privacy of individuals. A wealth of data being used within artificial intelligence constitutes personal data (Igglezakis [1]), while many of these data fall under special categories (Article 9(1) GDPR) (sensitive data). In this respect, for the functioning of artificial intelligence, the collection and processing of large data sets, which are difficult to place under the control of data subjects, is required. The reliance of artificial intelligence on data has created a critical paradox: while a greater volume of data enhances the accuracy of artificial intelligence outcomes, it also heightens the risk of privacy violations by malicious actors (Khatri [2]) seeking to retrieve sensitive information (Dilmegani [3]). Indeed, according to the Identity Theft Resource Center, in 2021 there were 1,862 data breaches – a rate that is 23% higher than the previous all-time high in 2017.In short, personal data feeds the artificial intelligence system, which, in turn, generates new, additional data. As the algorithm often outperforms its creator due to the latter's inability to comprehend how it operates, fulfilling the legal obligation of informing data subjects on how the algorithm functions (Articles 12 et seq. GDPR) is not always feasible. By extension, the same also applies to informing data subjects about the data being collected and the broader processing thereof. Bearing in mind the above, the fundamental principles of data processing (Article 5 GDPR) [4] appear to be put to the test. The aim of the present study is precisely to delve into the issues set out above.

Clarifications on Terminology

Artificial intelligence is the branch of computer science that deals with the design and implementation of computer systems that simulate elements of human behavior that assume at least a rudimentary level of intelligence: learning, adaptability, inference, contextual understanding, problem-solving, and so on (McCarthy [5]). Artificial intelligence refers to systems that demonstrate intelligent behavior by analyzing their environment and taking steps to achieve their goals [6] with a certain degree of autonomy. In this sense, artificial intelligence systems are designed by humans and are capable of perceiving and interpreting data from their environment, making optimal decisions and reproducing human cognitive functions such as learning, planning, and decision-making. The scientific discipline of artificial intelligence is comprised of several approaches and techniques:

a) Machine learning, of which deep learning and reinforcement learning are specific examples.

b) Machine reasoning, which includes planning, scheduling, knowledge representation and reasoning, search, and optimization.

c) Robotics, which includes control, perception, sensors, and actuators, as well as the integration of all other techniques into cyber-physical systems [7].

Artificial intelligence is contrasted with human intelligence, as it does not originate from living beings (Christodoulou [8]). In reality, it consists of automated, non-intermediated human decision-making through a sequence of logical actions resulting from machine learning/deep learning. Machine learning is divided into supervised and

unsupervised. In the first case, algorithms have been "trained" to draw conclusions based on data that have been input by their programmers [9]. On the reverse, under unsupervised machine learning, the algorithms have not been input and are left without guidance/pointers in drawing inferences [10]. Notwithstanding the above, it is crucial to point out the following:

(a) Machines do not act on their own, but imitate human behavior (Zekos [11]);

(b) The basis of knowledge derives from human effort;

(c) Machines do not learn on their own but are guided by us;

(d) They do not necessarily adopt racist prejudices, but they rely on racist patterns of human behavior, which they copy; and

(e) Machines do not think as humans, but they do act rationally (Yannopoulos [12]).

Artificial intelligence operates independently from its creator (Vlachopoulos [13]), making a prediction/estimation. The algorithm uses existing data to predict human behavior, for instance in order to determine whether a citizen has committed a certain violation. In such cases, algorithms are not linear and they are usually not interpretable, either: therefore, it is not always easy – or even possible – to know how each variable has made its contribution. This is more common in cases where the deep learning technique is used. In this context, artificial intelligence comes into existence when it is possible to go beyond the application of the rules set by the programmer for the algorithmic analysis of a large volume of data, with the program creating new rules from the correlations it identifies within the data provided (Menéndez Sebastián & Mattos Castañeda [14]). The distinguishment of artificial intelligence into strict intelligence, strong intelligence and superintelligence is sharper. Strict artificial intelligence focuses on solving specific problems based on purely mathematical methods. The strongest expression of artificial intelligence is modelled on the ability to mimic human beings and their inductive and cognitive capabilities. If the latter is exceeded, the outcome is a super-intelligence that is capable of surpassing humans themselves (Pica [15]).

The General Issue

The operation of artificial intelligence seems to come into strain with the underlying philosophy of data protection (Panagopoulou Koutnatzi [16]). The main tensions can be seen in the principles set out below and the right to human intervention.

The Purpose Limitation Principle

The application of the purpose limitation principle in the context of the operation of artificial intelligence systems presents a particular set of challenges. With regard to the data input for the purposes of deriving recommendations relating to a medical, administrative or other decision-making process, the principle in question is more easily applied. In such cases, the purpose of processing is specific and predetermined, hence it is considered necessary to take appropriate measures to ensure that the algorithm's processing is limited to what is required in order to achieve said purpose. The system must be restrained from extracting conclusions that are irrelevant, such as, for example, conclusions on fertility or the likelihood of developing prostate cancer, when the purpose of the processing is to interpret gastroenterological symptoms experienced by the patient. Nevertheless, this is not always straightforward, as it is often the case that certain parallels end up being drawn, which pertain to seemingly unrelated parameters. At the same time, in the event that the data are used retrospectively and for purposes beyond those initially envisaged, for example, in the context of the algorithm's machine learning process, it is necessary to re-inform the data subject, following Article 13(3) or 14(4) of the GDPR. Clearly, when it comes to multiple processing of a common data pool for multiple purposes, this becomes difficult.

The Data Minimization Principle

The intertwining of the operation of an artificial intelligence system with the principle of data minimization raises the question of the nature and scope of the personal data that will be entered into the system as a "query" for the purposes of extracting a response. Given that the artificial intelligence system will only process and take into account in its analysis those data that will be entered into it, it is reasonably argued that to obtain a more accurate result, it is absolutely necessary to enter as much information as possible concerning a given patient/person that is being administered, and so on. Indeed, this would appear to be the case even when it comes to information that is presumed to influence the position of such persons only indirectly or to an infinitesimal extent. In the indicative case of patients, this list may include information relevant to every aspect of the patient's life, ending up constituting an excellent psychogram of the patient in question. At the same time, it could be argued that it would be useful for the system to include health data on the patient's relatives or people whose living conditions are similar to those of the patient, such as neighbors, partners, and so forth, to enable the system to draw more accurate conclusions concerning the patient's health status through comparison.

This, in turn, gives rise to further questions relating to the provision of information and the obtaining of consent from data subjects. Although the principle of data minimization does not seem to be compatible with the operation of artificial intelligence, the adoption of specific strategies is deemed necessary to ensure that a system, such as a medical artificial intelligence system, does not register data that appear to be irrelevant to the health of the individual, such as data relating to political beliefs, trade union memberships or banking data. This distinction is not always easy to make, as correlations cannot always be excluded - for instance, those that may exist between income and health status, political convictions and vaccinations, and so on.

At this point, it should also be highlighted that the algorithm works better when it is provided with as much data as possible. Consequently, the optimal operation of artificial intelligence requires a de facto relaxation of the principle of data minimization.

The Storage Limitation Principle

Data entered into artificial intelligence systems in the form of a "query" for the purposes of making a proposal should be deleted or anonymized after this purpose has been served. If the data are kept in the system's database in a non-anonymized form, it is deemed that the purpose of the processing has changed, and it becomes necessary to re-inform the data subject and obtain his or her consent - which is something that is not easily done.

The Accuracy Principle

Special caution and diligence must be exercised in the process of entering data relating to patients, administrators and so on to formulate a certain opinion. In the field of health, in particular, the accuracy of this data is decisive for the soundness of the conclusions that are to be reached regarding the health of the data subject, as well as for drawing an accurate profile of the data subject, given that the algorithm will only take into account the data entered into it. In fact, the consequences of processing inaccurate or false data on the data subject are highly critical and may even pose a risk to life.

The Principle of Transparency

The principle of transparency seems to be called into question in the case of artificial intelligence. The information requirements imposed by Articles 13 and 14 of the GDPR are cumbersome, especially with regard to the metadata that have been entered into the system's database. The provision of information may not be comprehensive because of the difficulty in determining accurately and in advance the purpose of the processing, or due to the complexity of the purpose or of the processing from a technical point of view. In the case of medical artificial intelligence, the provision of general information on the processing of data for medical diagnosis and research may be considered sufficient. With reference to the period for which data are stored, it is not clear how long the data will be stored: the data will remain in the system's database and will be subject to processing for as long as it is necessary for serving the purpose of the processing. Therefore, where the purpose of the processing is not fully specified from the outset or if it is constantly changing, it is not possible to provide full and accurate information to the data subject as to the period of retention of his or her data. In some instances, this could be a long time, such as in the case of all images of a certain part of the body from 1900 onwards.

Further to any difficulties in providing information, particular emphasis should be placed on the obligation of the controller to explain the reasoning followed by the artificial intelligence system during the automated data processing, both prior to the processing in the context of informing the data subject under Articles 12 et seq. of the GDPR, as well as subsequent to it, in the event that the data subject exercises his or her right of access under Article 15 of the GDPR. In this regard, concerns are raised as to the actual possibility of the controller, or of any other person involved, informing the average person on how the highly complex information systems and artificial intelligence algorithms operate ([9,17]). In fact, certain artificial intelligence systems have achieved such a degree of autonomy that it has become particularly difficult, if not impossible, for their manufacturers or operators themselves to comprehend the system's operating mechanism, let alone explain it in a simple, clear, and accessible way to someone who does not possess the relevant technical knowledge. These are the so-called "black boxes", which are based on complicated and constantly evolving algorithms that surpass the capabilities of human control (Vorras, et al. [18,19] Reed, 2018). The concerns set out above could be addressed through the restrictions on information and access to data provided in the GDPR.

Special emphasis should be given to Article 14(5) of the GDPR, which stipulates that in cases where personal data have not been obtained from the data subject, the controller is not obliged to provide thorough information as provided in paragraphs 1-4 of the Article in question, when:" the provision of such information proves impossible or would involve a disproportionate effort […] or (if the information) is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases, the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available". At the same time, in accordance with Recital 63 of the GDPR: "That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software." This regulation could be broadly applied to artificial intelligence systems because of the inherent impossibility of providing full information to each data subject and the potential intellectual property rights of the software creator.

The Security Principle

Artificial intelligence systems are vulnerable to attacks (Comiter [20]). In particular, malicious actors can manipulate artificial intelligence systems to serve their own goals (Comiter [20]) of targeted information, misinformation, manipulation, surveillance, harassment, deception, and so on. While traditional cyber-attacks are usually caused by human errors in the configuration of the code and can be detected and remediated, artificial intelligence attacks stem from inherent limitations of the algorithms, which are currently not easily curable (Comiter [20]). This means that in the case of an attack on an artificial intelligence model, the problem originates from the algorithm itself and its dependence on data (Comiter [20]). As a consequence, attackers can "mutate" the data used to train artificial intelligence systems, influencing the decisions that they make (Finan-

cial Postman [21]). As many artificial intelligence applications relate to critical areas of everyday life, attacks have a significant impact on public security, information, privacy, and so forth.

The Objectivity Principle

In the context of the "ethical" and "fair" design of artificial intelligence systems and the interest of the general principles of objectivity, morality and justice, the design and operation of artificial intelligence algorithms must be tailored to the specificities of the population to which they refer and on which they are to be used. An artificial intelligence system in the field of health that is to be used in health structures in Greece ought to take into consideration the local origin of data. In many cases, climatic conditions are of considerable importance and, thus, a comparison with countries that have other characteristics may be inappropriate. Therefore, it would not be considered compatible to use a medical algorithm that has been "trained" with data from the "Western world" to draw conclusions concerning the health of patients in refugee camps in civil war-ravaged South Sudan or the slums of Sierra Leone (Khanjani [22]). Even so, this does not apply to all cases, as there may well exist global databases, too. At the same time, it is also crucial to introduce sufficient data into the system that also relates to population "minorities", such as refugees and immigrants, people with specific genetic characteristics or syndromes, and so on, as the existence of a "bias" in the operation of the medical artificial intelligence algorithm could lead to significant consequences for the patient's health: if the patient falls into one or more categories of characteristics that are underrepresented, the diagnosis produced by the algorithm may be incorrect or inaccurate due to a lack of data on which it relies. It is also possible that bias may be inherent in the algorithm used for recruitment purposes if it has been created by men.

The Right to Human Intervention

The right to human intervention comes in two forms: The first one prohibits the adoption and implementation of a decision based exclusively on the automated processing of personal data (Article 22(1) of the GDPR), which has the effect of requiring substantial human involvement in the processing even if the data subject does not specifically request it. The second one provides that even where a decision based solely on automated processing is allowed to be taken and implemented (Article 22(2) and 22(4) of the GDPR), the data subject retains the right to request human intervention (Article 22(3) of the GDPR).As regards medical artificial intelligence systems, it should be stressed that, for the time being, they are used in such a way as not to make a final decision concerning the patient themselves (Article 62(4)(j) of Regulation (EU) 2017/745); instead, they provide a sort of "recommendation" or "opinion" to the attending physician, who is responsible for making the final decision on the diagnosis and treatment of the patient. Consequently, the decision on the treatment of an ailment made using the system is, in principle, designed so as not to fully automate the processing of the patient's data. Hence, even though the data are processed by the algorithm, the physician in charge is called upon to actively participate in the process of formulating the diagnosis and deciding on the appropriate therapeutic approach. To begin with, the physician is required to provide an opinion on the accuracy and correctness of the algorithm's results. Naturally, some doubts arise as to the physician's genuine ability to assess the results of the algorithm, let alone the process of extrapolating them, mainly due to the highly technical nature of these procedures.

As a result, a physician cannot be reasonably expected to be able to comprehend them. Consequently, it may be extremely difficult, if not impossible, for a medical practitioner to make an assessment as to the correctness of the diagnosis provided by the artificial intelligence algorithm or on the process of its extraction, even when the system is capable of justifying its decision automatically. Nevertheless, the physician can express a clinical opinion through non-automated processing of all the data contained in the medical record. It is therefore up to the medical practitioner to review the patient's file, to justify the diagnosis he or she comes to and, finally, to approach the case in a manner similar to the procedure that he or she would follow if it were not for the "assistance" provided by artificial intelligence algorithms. This approach is necessary since the use of an artificial intelligence system by medical practitioners does not relieve them of their personal liability for medical errors or negligence under currently applicable legislation. In the opposite case, that is, if the physician does not actively proceed to an assessment of the patient's condition and, instead, "blindly" follows the algorithm's advice by simply stating that he or she is in agreement with it or reiterates any justification offered by the algorithm, relying on the credibility of the machine, the (human) intervention on the part of the physician in the processing of the data is not deemed sufficient. As a result, the decision taken is, as a matter of fact, based solely on the automated processing of the data performed by the algorithm, thus activating the provisions of Article 22(2)-(4) of the GDPR.

Said provisions stipulate that where the patient has provided legally valid consent to the making of a decision based solely on automated processing (Article 12 of Greek Law No. 3418/2005, Code of Medical Ethics) or where this is necessary for reasons of substantial public interest under European or national law, following Article 22(4) of the GDPR, the lawfulness of the processing shall not be affected. Indeed, this holds true even though the data subject retains the right to subsequently request intervention on the part of the physician by way of exercising the corresponding right under Article 22(3) of the GDPR. If this were not to be the case, the non-decisive intervention and contribution of the physician in the processing of the data and the decision-making process renders the taking of the decision in question contrary to the GDPR. Therefore, under the GDPR regime, the use of artificial intelligence systems must be solely auxiliary to the process of assessing the patient's state of health and choosing the most suitable treatment.

Lastly, when the physician's personal assessment regarding the patient's state of health is not in agreement, in whole or in part, with the result provided by the algorithm, the question as to which opinion should prevail arises: will it be that of the algorithm's diagnosis or the physician's? When the data processing is not exclusively automated from the outset, the physician's opinion takes de facto priority. Where the decision can be legitimately based on exclusively automated data processing, for instance where the patient has consented to such processing, it is more appropriate to, once again, offer the patient the option of choosing which of the alternative approaches (i.e. that of the physician or the algorithm) is to be applied, since this option is always possible. After all, in emergency situations, a process of decision-making may take place to classify, categorize and triage patients based on medical criteria. If the patient is not in a position to choose, the attending physician will be faced with yet another dilemma: respect the patient's wish that the algorithm's suggested approach be applied unconditionally or follow the treatment that he or she deems appropriate?

Does Artificial Intelligence Overthrow the Fundamental Principles of Data Protection?

A further issue that emerges is whether algorithmic decision-making overthrows fundamental principles of data protection. It is evident from the foregoing discussion that the core principles of data protection law can delineate the boundaries of algorithmic decision-making. This means that the algorithm should not use data beyond what is necessary, delete unnecessary data or anonymize them; be defined, operate for a specific purpose, rely on data that is accurate, adhere to the principle of proportionality, and so on. This can be achieved if the algorithm is specific, definable, comprehensible and assists, rather than replaces, civil servants, physicians, and judges (Panagopoulou [23]). Nevertheless, the question posed above could well be reversed: is the currently established law on data protection capable of meeting the challenges presented by new technologies or does it constitute an "obstacle" for new developments? The answer to this question is complex. It is true that established data protection principles tend to give priority to data protection rights over corresponding information and research rights (Panagopoulou Koutnatzi, [24]). For this reason, the regulation of artificial intelligence calls for a holistic approach from the point of view of data protection, as well as from that of the free flow of information, and the advancement of technology and research [25-27].

Concluding Remarks

From the above overview, it is evident that artificial intelligence presents a considerable challenge to the protection of privacy. This challenge does not suggest that artificial intelligence constitutes a violation of privacy, but rather that privacy law should be an important dimension of the regulation of artificial intelligence. In other words, it is an essential aspect of its regulation, but not the sole one. Privacy is a subsidiary issue of artificial intelligence, which is precisely why the monitoring of artificial intelligence calls for the establishment of an authority that will operate harmoniously alongside the Data Protection Authority, but will also have other areas under its remit, such as information, innovation, research, intellectual property, health, and so forth.

References

1. Igglezakis D (2022) The Law of Digital Economy. Sakkoulas Publications: Athens-Thessaloniki.
2. Khatri M (2023) Data Privacy in the Age of Artificial Intelligence (AI).
3. Dilmegani C (2024) Responsible AI: 4 Principles & Best Practices in 2024. AI Multiple Research.
4. General Data Protection Regulation (GDPR), Article 5; Article 9(1); Article 12.
5. McCarthy J (2017) What Is Artificial Intelligence.
6. (2018) European Commission. A Definition of Artificial Intelligence: Main Capabilities and Scientific Disciplines. The European Commission's High Level Expert Group on Artificial Intelligence.
7. (2018) European Commission. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe.
8. Christodoulou KN (2019) Legal Issues Arising from Artificial Intelligence. In Law and Technology, 22nd Scientific Symposium of the University of Piraeus and the Court of Audit. In: Delouka Igglesi KA, Ligomenou, A Sinanioti Maroudi (Eds.)., Sakkoulas Publications: Athens-Thessaloniki.
9. (2017) ICO. Big Data, Artificial Intelligence, Machine Learning and Data Protection.
10. Alpaydin E (2020) Introduction to Machine Learning. MIT Press.
11. Zekos GI (2022) The Internet and Artificial Intelligence in Greek Law. Sakkoulas Publications: Athens-Thessaloniki.
12. Yannopoulos G (2022) Presentation at a Webinar of the European Bioethics, Technoethics and Law Workshop on Artificial Intelligence.
13. Vlachopoulos S (2023) The 'Selfish Gene of Law' and the Law of Artificial Intelligence. In From Anthropocentrism to Ecocentrism and Intelligent Algorithms. Athens, Eurasia.
14. Menéndez Sebastián EM, BM Mattos Castañeda (2022) Better Decision-Making, Algorithmic Discrimination and Gender Biases: A New Challenge for the Administration of the 21st Century. European Review of Digital Administration & Law Erdal 3(1): 45-56.
15. Pica LM (2022) Artificial Intelligence Tax Law and (Intelligent?) Tax Administration. European Review of Digital Administration Law Erdal 3(1).
16. Panagopoulou Koutnatzi F (2023) Artificial Intelligence: The Road Towards Digital Constitutionalism. An Ethico-Constitutional Consideration. Athens: Papazisis Publications.
17. (2016) EDPS. Artificial Intelligence, Robotics, Privacy and Data Protection. Room Document for the 38th International Conference of Data Protection and Privacy Commissioners.
18. Vorras A, L Mitrou (2018) Artificial Intelligence and Personal Data - A Consideration in the Light of the European General Data Protection Regulation (EU) 2016/679. Journal of Technology and Communications Law.

19. Ferretti A, Schneider M, Blasimme A (2018) Machine Learning in Medicine: Opening the New Data Protection Black Box. EDPL 4(3): 320-322.

20. Comiter M (2019) Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It. Harvard Kennedy School, August.

21. (2023) Financial Postman. Artificial Intelligence: What could 'throw it up in the air.

22. Khanjani N (2016) Climate Parameter Variability and Health. In Topics in Climate Modeling.

23. Panagopoulou F (2024) Algorithmic Decision-Making in Public Administration. Journal of Public Administration 6(1).

24. Panagopoulou Koutnatzi F (2019) Constitutional View of the Law on Protection of the Environment. Journal of Technology and Communications Law 328 et seq.

25. Greek Law No. 3418/2005 (Code of Medical Ethics), Article 12.

26. Regulation (EU) 2017/745 on Medical Devices, Article 62(4)(j).

27. Regulation (EU) 2017/746 on *In Vitro* Diagnostic Medical Devices.

ISSN: 2574-1241

DOI: 10.26717/BJSTR.2024.55.008761

Fereniki Panagopoulou. Biomed J Sci & Tech Res