**Maria Jędrzejczak**
Adam Mickiewicz University in Poznań, Poland
maria.jedrzejczak@amu.edu.pl
ORCID: 0000-0002-9384-7096

https://doi.org/10.26881/gsp.2024.3.07

# Protection of Personal Data Processed in Artificial Intelligence Systems

## Introduction

European legal reality is on the eve of significant change. In European Union (EU) law, there is talk of a "fourth industrial revolution," which is driven by massive data resources linked to powerful algorithms and powerful computing capacity.[1] The above is closely linked to technological developments in the area of artificial intelligence (AI), which has prompted an analysis covering both the legal environment as well as the economic and social impact, also from an ethical perspective.[2]

The discussion on the regulation of artificial intelligence is one of the most serious and widely held at both EU and Member State level. The literature expects legal solutions to guarantee security for fundamental rights, including privacy, in AI systems.

There is no doubt that personal data have been increasingly processed in recent years. It would be impossible for AI to function without processing large amounts of data (both personal and non-personal[3]). Artificial intelligence is a collection of technologies that combine data, algorithms, and computing power. The main driving force behind the current development of AI is advances in computing, but also the increasing availability of data. High-quality data are crucial to the effectiveness of many AI systems, particularly when using techniques involving model training.[4] The

[1] See European Parliament resolution of 3 May 2022 on artificial intelligence in a digital age (2020/2266(INI)), https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_EN.html [accessed: 2023.08.31].

[2] The most important ethical guidelines for AI are considered to be: transparency, justice and fairness, non-maleficence, responsibility, and privacy. A. Jobin, M. Ienca, E. Vayena, *The global landscape of AI ethics guidelines*, "Nature Machine Intelligence" 2019, No. 1(9), pp. 389–399.

[3] As an aside, it should be pointed out that distinguishing personal data from non-personal data can cause significant difficulties in practice. The capabilities of AI systems - using data flows, combining data from different sources, aggregating or creating datasets - are pushing the boundary between personal and non-personal data. More extensively on this topic: B. Fischer, *Prawne uwarunkowania wykorzystania danych nieosobowych przez sztuczną inteligencję – zagadnienia podstawowe* [in:] *Prawo sztucznej inteligencji i nowych technologii 2*, eds. *idem*, A. Pązik, M. Świerczyński, Warszawa 2022, p. 181.

[4] Recital 45 of the draft AI Act further indicates that in order to develop and assess high-risk AI systems, certain actors, such as suppliers, notified bodies and other relevant entities, including digital

use of computers and AI technology allows for an increase in the speed and efficiency of the actions taken, but also creates security risks of an unprecedented magnitude for the data processed.

The proposed regulation in the field of AI requires analysis in terms of its impact on the regulation of personal data protection. It is necessary to determine what the mutual relationship between these regulations is and what areas are particularly important in the personal data protection regulation for processing personal data in AI systems. The axis of considerations adopted is a preliminary assessment of two issues: 1) what principles of data protection should be applied in particular during processing personal data in AI systems; 2) what regulation on liability for personal data breaches is in such systems. However, only after EU regulation on AI comes into force and the use of AI systems is widespread, will it be possible to outline the exact legal problems. The need to change the regulations regarding the rights and obligations of data subjects and entities processing personal data cannot be excluded. It is possible that changes will be required in the provisions regarding the assignment of liability for a breach of personal data protection processed in AI systems, which is discussed in more detail in the last point of this article.

Given the relatively short experience of European countries in the application of AI and the absence – at the time of writing – of a binding legal instrument dedicated to AI issues and case law in this area, the present study will be of a contributory nature, prompting further discussion. The research process in this case concerns the identification of areas in the field of personal data protection that are particularly important (and may require re-regulation) as a result of the introduction of the proposed legal regulation regarding AI. The main question this article seeks to answer is how EU regulation against data protection breaches in AI systems is shaping up.

## 1. Artificial intelligence regulation assumptions

The EU has taken steps to regulate the European approach to artificial intelligence issues in, inter alia, the White Paper on Artificial Intelligence "A European Approach to Excellence and Trust" (hereinafter referred to as the White Paper).[5] This policy paper identifies the European Commission's main intentions for structuring legislation in the area of artificial intelligence. In particular, it has been pointed out that the White Paper creates: 1) a policy framework outlining measures to combine efforts at European, national, and regional levels; 2) key elements of a future regulatory framework for AI in Europe that will create a unique "ecosystem of trust."

innovation centres, test and experiment centres and researchers, should be able to access and use high-quality datasets in their areas of activity.

[5] European Commission, White Paper on Artificial Intelligence. A European Approach to Excellence and Trust, COM(2020) 65 final, Brussels, 19.02.2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0065 [accessed: 2023.08.31].

The areas of action presented in the White Paper complement the plan presented in parallel in the European Strategy for Data.[6] It has been pointed out that improving access to data and data management are a critical issue, as without data, AI development is not possible. The importance of investment in computing technology and infrastructure has also been also highlighted. As part of the Digital Europe programme, the European Commission has proposed more than EUR 4 billion to support large-scale and quantum computing, including grid edge computing and artificial intelligence, data infrastructure, and cloud computing.

The European Commission has stressed the importance of shaping the European approach to AI in such a way that it is characterised by the implementation of appropriate safeguards to respect fundamental rights and freedoms, the development of trustworthy and secure AI and respect for the values underlying the EU, including the principle of privacy. Highlighting these aspects of AI systems within the EU shows a desire to counter the approaches of the other two major global players in the field of artificial intelligence: China and the USA.[7]

The most important piece of legislation in the area of artificial intelligence is the draft regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (hereinafter referred to as the draft AI Act[8]) published on 21 April 2021.[9] Among other things, the draft introduces a legal definition of artificial intelligence. According to the original wording in Article 3(1) of the draft AI Act, an AI system was defined as "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with." In turn, Annex I indicates that AI may include:

1) machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
2) ogic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;
3) statistical approaches, Bayesian estimation, search and optimization methods.

After changes to the draft AI Act, adopted by the European Parliament, an AI system is defined as "machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs

[6] European Strategy for Data, https://digital-strategy.ec.europa.eu/en/policies/strategy-data [accessed: 2023.08.31].

[7] As pointed out in the White Paper, investment in research and innovation in Europe represents a small proportion of public and private investment compared to other regions of the world. In 2016, around EUR 3.2 billion was invested in AI in Europe, while around EUR 12.1 billion was invested in North America and around EUR 6.5 billion in Asia.

[8] The European Parliament adopted the draft AI Act in March 2024 and the Council followed with its approval in May 2024. The regulation was published on July 12, 2024 and is waiting to come into force.

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206 [accessed: 2023.08.31].

such as predictions, recommendations, or decisions, that influence physical or virtual environments."[10] The EU legislator abandoned the definition focused on listing specific techniques that can be used by AI (e.g. machine learning) in favor of defining the basic features that characterize AI (e.g. autonomy).

This definition covers a wide set of AI systems that will be subject to the proposed regulation, which is intended to reduce the chance of its becoming obsolete. However, the proposed solution poses the risk of over-regulation, which will hinder the use or development of artificial intelligence applications, which is likely to further strengthen the technological leadership position of Chinese and US corporations.[11]

However, it should be emphasised that providing such a comprehensive definition serves to better guarantee the safe operation of AI systems within the EU. The technological capabilities and the willingness of the authorities of some states, including authoritarian states, to make the widest possible use of advanced technology have led to a point where possible abuses can only be analysed on the basis of human rights regulations. The human rights protection system often remains an inadequate tool, too general and failing to provide adequate compliance mechanisms.[12] The draft AI Act has the potential to become the first legal tool to give EU citizens better protection of their rights and interests.

## 2. Guidelines for personal data protection in AI systems

One of the main problems noted when analysing AI regulation is the issue of the potential for infringement of the right to privacy. The European Parliament has rightly pointed out that some AI technologies enable the automation of information processing on an unprecedented scale, paving the way for mass surveillance and other unlawful interference and threatening fundamental rights, in particular the right to privacy and data protection.[13]

---

[10] Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html [accessed: 2024.02.07].

[11] P. Glauner, *An Assessment of the AI Regulation Proposed by the European Commission* [in:] *The Future Circle of Healthcare. Future of Business and Finance. AI, 3D Printing, Longevity, Ethics, and Uncertainty Mitigation*, eds. S. Ehsani, P. Glauner, P. Plugmann, F.M. Thieringer, Cham 2022, pp. 119–127.

[12] "In a world where new technologies fundamentally change social relations and practices, it is not always clear what human rights and the rule of law actually mean, and how respect for human rights can be safeguarded" – F. Bosco, N. Creemers, V. Ferraris, D. Guagnin, B.-J. Koops, *Profiling technologies and fundamental rights and values: regulatory challenges and perspectives from European Data Protection Authorities* [in:] *Reforming European Data Protection Law*, eds. S. Gutwirth, R. Leenes, P. de Hert, Dordrecht 2015, pp. 3–33.

[13] European Parliament resolution of 3 May 2022 on artificial intelligence in a digital age (2020/2266(INI)), Report on Artificial Intelligence in a Digital Age, https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1703188&t=d&l=en [accessed: 2023.08.31].

In view of the above, it is necessary to analyse the regulations applicable in this respect. Recital 41a of the draft AI Act indicates that "a number of legally binding rules at European, national and international level already apply or are relevant to AI systems today, including […] EU secondary law (such as the General Data Protection Regulation […]." Thus, the AI Act is intended to be a supplementary regulation to the General Data Protection Regulation (GDPR),[14] which is to remain the basis for the horizontal compatibility assessment of AI systems in the area of personal data.[15]

Several provisions can be found in the draft AI Act that address the issue of handling personal data processed in AI systems. Article 10 of the AI Act sets out rules for the handling of training, validation and testing data sets used by high-risk AI systems. It is pointed out that "to the extent that it is strictly necessary for the purposes of ensuring negative bias detection and correction in relation to the high-risk AI systems, the providers of such systems may exceptionally process special categories of personal data […] subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving" (Article 10(5) of the draft AI Act).

In turn, Article 53 of the draft AI Act, relating to so-called AI regulatory sandboxes, guarantees national data protection authorities, or in cases referred to in Article 53(1b) the European Data Protection Supervisor, access to the activities of such a regulatory sandbox (Article 53(2) of the draft AI Act).

In contrast, Article 60 of the draft AI Act indicates what personal data will be processed in EU databases for high-risk AI systems (primarily the names and contact details of the individuals who are responsible for registering the system and have the authority to represent the provider or the deployer, which is a public authority or EU institution, body, office or agency, or a deployer acting on their behalf, or a deployer which is an undertaking referred to in Article 51(1a)(b) and (1b), without defining specific rules for their protection.

The EU legislator has not separately regulated data protection in any of the above cases. One of the key issues requiring in-depth analysis is, therefore, the potential collision of AI systems with privacy and data protection. The GDPR regulates profiling and automated forms of decision-making in individual cases, which are forms of processing that are also part of many AI-based models.[16] There is no doubt that the EU's data

[14] 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) (OJ EU L 119, p. 1).

[15] D. Lubasz, A. Szkurłat, *Relacja aktu o sztucznej inteligencji i ogólnego rozporządzenia o ochronie danych*, "Monitor Prawniczy" 2022, No. 21, p. 28. Significantly, the European Parliament stated that "GDPR does not seem to require any major change in order to address AI." European Parliament, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf [accessed: 2023.08.31].

[16] More extensively on this topic: M. Jędrzejczak, *Automatyzacja wydawania rozstrzygnięć administracyjnych – nieprecyzyjność przepisów jako zagrożenie dla ochrony danych osobowych* [in:] *Ochrona danych osobowych w prawie publicznym*, ed. *eadem*, Warszawa 2021, pp. 61–75.

protection standard, as set by the GDPR legislation, is one of the most stringent in the world. Despite this, the development of AI-based technologies raises legal questions. In this context, the compatibility of AI models with the GDPR regulation needs to be verified, and directions for potentially required modifications to the legal environment need to be set, taking into account processing principles that correlate with the basic tenets of the development of trustworthy AI.

The principles relating to the processing of personal data are regulated in Article 5 of the GDPR and include the principles of lawfulness, fairness, and transparency, the principle of purpose limitation, data minimisation, accuracy, limitation of storage, integrity and confidentiality, and the principle of accountability. The principles override and form the core of the interpretation of the other provisions of the GDPR. They also aim to ensure the least possible interference with fundamental rights.

From the perspective of the design of AI systems, it will be important to ensure compliance with the processing principles that set the general framework for the permissibility of data use in the design of AI solutions.[17] In this respect, the principles of lawfulness, transparency, data minimisation, and confidentiality are particularly relevant.[18] Due to the framework of the study, those principles were selected that may cause the most difficulties for entities using AI-based mechanisms in their activities. At the same time, these are principles that correspond to the basic assumptions of constructing trustworthy AI, indicated in the documents of the Organisation for Economic Co-operation and Development (OECD)[19] or the High-Level Expert Group on AI.[20]

### 2.1. Principle of lawfulness and transparency (Article 5(1)(a) of the GDPR)

The principle of lawfulness (legality) is an overarching principle that applies as a universal limit to all actions, including discretionary actions[21] (the operation of AI systems, even for developers, is not fully understood and therefore remains difficult to control, as does discretion). This principle has a broad material scope – it is a question of compliance with all provisions that may be applicable to the case (not only the provisions of the GDPR). Processors of personal data have certain obligations that they should comply with and data subjects are guaranteed certain rights that should be respected.[22]

---

[17] Also: D. Lubasz, *Zasady legalności, przejrzystości i minimalizacji danych w ogólnym rozporządzeniu o ochronie danych osobowych w kontekście sztucznej inteligencji* [in:] *Prawo sztucznej inteligencji*, eds. L. Lai, M. Świerczyński, Warszawa 2020, p. 180.

[18] The CJEU's view that all principles relating to the processing of personal data shall apply cumulatively should be shared. Judgment of the CJEU of 20 October 2022 in Digi Távközlési és Szolgáltató Kft. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, C77/21, ECLI:EU:C:2022:805.

[19] OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, https://oecd.ai/en/assets/files/OECD-LEGAL-0449-en.pdf [accessed: 2024.02.07].

[20] High-Level Expert Group on AI, *Ethics guidelines for trustworthy AI*, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai [accessed: 2024.02.07].

[21] M. Jędrzejczak, *Władza dyskrecjonalna organów administracji publicznej*, Warszawa 2021, p. LVIII.

[22] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia*

Analysis by those creating or using AI systems should be directed not only to the application of a legal basis appropriate to the source of data acquisition, but also to the design of AI algorithms or systems in such a way as to ensure the correctness and non-discriminatory nature of the processing and the effect of such operations, in particular biased adjudications, affecting the rights and freedoms of data subjects.[23] The AI system should ensure that the data are processed in a way that the data subject can expect the result to be. In addition, such technical measures should be implemented as to ensure the correction of irregularities and the safeguarding of personal data.

On the other hand, the transparency principle, also expressed in Article 5(1)(a) of the GDPR, stresses an obligation to ensure that data subjects have the fullest possible knowledge of the purpose, scope, and context of the processing, as well as the possibility of exercising control over their own data. In the context of AI systems, an essential condition for compliance with this principle is to communicate that it is the AI-based system that will process personal data. It is not advisable, and sometimes not possible, to explain in detail the technical intricacies involved in the operation of a given AI system (especially if it is based on deep learning).[24] It is important to ensure awareness of being subjected to such forms of processing in order to be able to fully exercise rights of control over one's own data.

### 2.2. Principle of data minimisation (Article 5(1)(c) of the GDPR)

The data minimisation principle states that only personal data which are necessary for the purposes for which they are processed may be processed by the controller. The amount and scope of the data to be collected and processed must be adequate and appropriate to achieve the purpose of the processing. This demonstrates the close relationship between the principle of minimisation and the principle of purpose limitation, which determines the adequate scope of the data to be collected. This is because it is the purpose of the processing that will determine what data are necessary to achieve it. This relationship must be able to be demonstrated and justified by the controller.

This principle will apply to AI systems in both the learning processes and their applications. The main difficulty at the learning stage is that at the data acquisition stage, AI developers cannot always predict how much data will be required to achieve a satisfactory learning outcome. At the application stage of the algorithm, it can be problematic to achieve a sufficient threshold of comparable data to allow comparison with, for

---

*dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – Komentarz do art. 5* [in:] *idem*, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022.

[23] D. Lubasz, M. Namysłowska, *Zasady dotyczące przetwarzania danych osobowych a sztuczna inteligencja w kontekście europejskim* [in:] *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, eds. K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Warszawa 2019.

[24] This is also what the CJEU pointed out in a recent judgment, emphasising that "the principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used." Judgment of the CJEU of 12 January 2023 in RW v. Österreichische Post, C154/21, ECLI:EU:C:2023:3.

example, a statistical model in order to draw a valid conclusion, which will indirectly overlap with the requirements under the principle of accuracy.

In both of the above cases, it can be extremely difficult to draw the line between adequate and inadequate data, and it can be even more difficult to demonstrate this relationship based on measurable criteria.

### 2.3. Principle of confidentiality (Article 5(1)(f) of the GDPR)

In accordance with the principle of confidentiality and integrity, data must be processed in a manner that ensures adequate security. Data security – both technical and organisational – is an important aspect of data protection in its broadest sense.

Ensuring adequate security requires that appropriate (proportionate) data security measures are taken. These do not have to be the best possible measures (e.g. the most technologically advanced), but they should be appropriate to the risks and allow effective protection.

In AI systems, compliance with the principle of confidentiality is particularly important, as the EU legislator explicitly emphasises. The draft AI Act refers to this principle several times (see, inter alia, Article 10, Article 30(6) and Article 70(1) of the draft AI Act). It is emphasised that cooperation between competent authorities at EU and national level should be based on respect for the principle of confidentiality of information and data obtained in the performance of their tasks (recital 83 of the draft AI Act).

Undoubtedly, maintaining an appropriate level of security, particularly technical security, for data processed in AI systems will be key to building trust in this technology with its users. However, it seems that controlling the correct implementation of this principle in practice, for technological reasons, may be difficult.

## 3. Liability for data breaches by AI

The issue of liability for breaches of data processed in AI systems also requires separate analysis. The comprehensive regulation of the GDPR provides for civil liability (compensation), administrative liability (administrative fines), and criminal liability (for unlawful processing of personal data) for breaches of personal data protection. The above should also apply to data processed in AI systems.

Some data protection breaches are closely linked to the use of modern information processing technologies. This includes, among others, the lack of adequate technical safeguards or the breaking of these safeguards. It is necessary to ensure the security and control of not only the AI algorithm itself, but also, among other things, Internet connectivity services, IoT end devices, and the security of the cloud used. Algorithmic accountability cannot be static; it must be looked at in dynamic terms, as many factors affecting security are subject to change, including in real time.[25]

[25] D. Szostek, *To nie takie proste. System odpowiedzialności za algorytmy, w tym AI, z perspektywy prawa unijnego* [in:] *Prawo sztucznej inteligencji*…, p. 125.

However, the most important task in this regard is to determine who (what entity) is liable for any data breach in AI systems.[26] Under the GDPR, it is the controller – the entity that alone or jointly with others determines the purposes and means of the processing of personal data – that bears the ultimate responsibility, whereas if a processor has been appointed, the responsibility should be apportioned in a manner proportionate to the degree of fault between the controller and the processor.

In this regard, the predecessor act to the draft AI Act was a European Parliament resolution with recommendations to the Commission on a civil liability regime for artificial intelligence.[27] It proposes to make the individuals who create, maintain, or control AI risks, in particular AI system operators, liable.

In the draft AI Act, "operator" means supplier, user, authorised representative, importer, and distributor. In this respect, the draft is in line with the recommendations of the resolution, as the main entity with assigned liability for the AI system is the supplier (one of the operators), i.e. the natural or legal person, public authority, agency, or other entity that develops the AI system or that has it developed with a view to placing it on the market or putting it into service under its own trade name or its own trademark; whether in return for payment or free of charge (Article 3(2) of the draft AI Act).

Recital 53 of the draft AI Act indicates that a specific natural or legal person identified as a supplier should be held liable. For high-risk AI systems, manufacturers (Article 24 of the draft AI Act), importers (Article 26(4) of the draft AI Act), and distributors (Article 27(3) of the draft AI Act) are also liable. In the cases set out in Article 28(1) of the draft AI Act, obligations equivalent to those of the supplier are also imposed on the user or other third party. Thus, in general, it is the operator (and in particular the supplier) who is responsible for the operation of the AI system, including possible breaches of protection of the data processed by the system.

In this context, one should also mention the EU proposal for an Artificial Intelligence Liability Directive.[28] Its provisions would only apply to non-contractual civil liability. However, they do not regulate the matter of contractual liability, so it must be assumed that the general rules, with freedom of contract at the forefront, will apply in this case. The draft directive envisages the introduction of a presumptive fault

[26] It should be added that it is not envisaged that AI can be granted legal personality and, therefore, there is no possibility of attributing to it liability for any infringements it may make. In the policy adopted for the development of artificial intelligence in Poland from 2020, "counteracting the granting legal personality to AI" is indicated as one of the objectives. See Annex to Resolution No. 196 of the Council of Ministers of 28 December 2020 on the establishment of the "Policy for the development of artificial intelligence in Poland from 2020" (M.P. 2021 item 23), https://wp.oecd.ai/app/uploads/2021/12/Poland_Policy_for_Artificial_Intelligence_Development_in_Poland_from_2020_2020.pdf [accessed: 2023.08.31].

[27] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)).

[28] Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (Artificial Intelligence Liability Directive), 2022/0303(COD), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496 [accessed: 2023.08.31].

construction of the defendant (supplier, user) for damages caused by high-risk AI systems.

## Concluding remarks

Analysing the provisions of the draft AI Act is currently a challenge as it concerns systems whose operation is not fully known and therefore not controllable. Any guidelines and arrangements in this area will be difficult to enforce in practice. Even the best legally drafted act will not guarantee data security in AI systems until it is possible to fully control the operation of these systems.

This is not an isolated reflection. The European Parliament, in its resolution, also pointed out that the opacity and autonomy of AI systems could make it very difficult or even impossible in practice to trace back specific harmful actions of the systems to specific human input or human decisions at the system design stage.[29]

The regulations contained in the draft AI Act are in the nature of demands, the implementation of which may not be possible in practice. The question of assigning liability to specific entities (e.g. suppliers) will need to be considered for the actions of AI systems, which they will not be able to effectively influence or correct. If it turns out for some AI systems that they operate beyond human control, the assumption of not giving legal personality to AI may have to be verified. Such a solution, however, is undesirable at the EU level and, secondly, would create further significant legal problems, e.g. regarding the conditions necessary to attribute legal personality to an AI system (not every system is equally autonomous[30]) and the question of how such a system is to be held liable (e.g. the possibility for AI to incur fines).

Another option would be to consider restricting the release of high-risk AI systems within the EU until effective methods of controlling them have been found.[31] There is no doubt that successful implementation of the AI Act requires prior knowledge of how the technology works. As a first step, AI systems must cease to be a "black box,"[32] whose complexity, unpredictability, and partly self-contained operation may make it impossible to enforce existing laws protecting fundamental rights, assigning liability, and setting out the conditions necessary for redress. The above requires an appropri-

---

[29] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)).

[30] More extensively on the autonomy of AI systems: S. Russell, P. Norvig, *Artificial Intelligence. A Modern Approach. Third Edition*, New Jersey 2016, pp. 39–40.

[31] In particular, this solution would be desirable during the development of so-called Strong AI or Artificial General Intelligence. More on this topic: G.W. Ng, W.C. Leung, *Strong Artificial Intelligence and Consciousness*, "Journal of Artificial Intelligence and Consciousness" 2020, Vol. 7, No. 1, pp. 63–72.

[32] Many approaches exist to providing explanations of the behaviour of neural networks and other opaque systems (also called black boxes). However, advancements of human-understandable explanation of neural networks are so far still quite limited. R. Guidotti, A. Monreale, S. Ruggieri, F. Turini, D. Pedreschi, F. Giannotti, *A survey of methods for explaining black box models*, "ACM Computing Surveys" 2018, Vol. 51, Issue 5, article 93.

ate period of trial and testing, which should take place in a way that is the least severe for society, thus excluding the use of high-risk AI systems in sensitive areas (especially in the public sector).[33]

The proposed solutions indicated in the AI Act should be enforceable; this is a prerequisite for the implementation of AI systems in the EU. The regulations adopted in this area and AI technology should inspire widespread confidence. Meanwhile, recent research indicates that the level of trust in AI is relatively low among the citizens of European countries.[34] The results of ongoing research also confirm that the role of trust in the acceptance of AI technology, including the intention to use it, is significant.[35]

The development of AI systems seems inevitable. It is the task of the legislator and lawyers to ensure that this technology is implemented as smoothly as possible, guaranteeing respect for fundamental rights, which are an undeniable value of European legal culture.

## Literature

Bosco F., Creemers N., Ferraris V., Guagnin D., Koops B.-J., *Profiling technologies and fundamental rights and values: regulatory challenges and perspectives from European Data Protection Authorities* [in:] *Reforming European Data Protection Law*, eds. S. Gutwirth, R. Leenes, P. de Hert, Dordrecht 2015.

Choung H., David P., Ross A., *Trust in AI and its role in the acceptance of AI technologies*, "International Journal of Human-Computer Interaction" 2022, Vol. 39, Issue 9.

Glauner P., *An Assessment of the AI Regulation Proposed by the European Commission* [in:] *The Future Circle of Healthcare. Future of Business and Finance. AI, 3D Printing, Longevity, Ethics and Uncertainty Mitigation*, eds. S. Ehsani, P. Glauner, P. Plugmann, F.M. Thieringer, Cham 2022.

Guidotti R., Monreale A., Ruggieri S., Turini F., Pedreschi D., Giannotti F., *A survey of methods for explaining black box models*, "ACM Computing Surveys" 2018, Vol. 51, Issue 5.

Fajgielski P., *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – Komentarz*

[33] In this respect, the deletion of Article 5(3) of the draft AI Act, which allowed – under certain conditions – remote biometric identification in public spaces, should be considered correct. More on concerns about deleted Article 5(3): M. Veale, F. Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach*, "Computer Law Review International" 2021, No. 4, p. 102.

[34] Research conducted by the University of Queensland with KPMG in 2023 shows that among the 17 countries participating in the survey on the level of trust in AI, European countries ranked at the bottom of the list. The highest levels of confidence in AI were demonstrated by: India, China and the Republic of South Africa. By contrast, among European countries, Germany was ranked 7th (35% of respondents showed confidence in AI), the UK 10th (34%), France 13th (31%), the Netherlands 14th (29%), Estonia 15th (26%) and Finland 17th (16%). See: *Trust in Artificial Intelligence. A global study 2023*, https://assets.kpmg.com/content/dam/kpmg/au/pdf/2023/trust-in-ai-global-insights-2023.pdf [accessed: 2023.08.31].

[35] H. Choung, P. David, A. Ross, *Trust in AI and its role in the acceptance of AI technologies*, "International Journal of Human-Computer Interaction" 2022, Vol. 39, Issue 9, pp. 1–13.

*do art. 5* [in:] *idem*, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022.

Fischer B., *Prawne uwarunkowania wykorzystania danych nieosobowych przez sztuczną inteligencję – zagadnienia podstawowe* [in:] *Prawo sztucznej inteligencji i nowych technologii 2*, eds. *idem*, A. Pązik, M. Świerczyński, Warszawa 2022.

Jędrzejczak M., *Automatyzacja wydawania rozstrzygnięć administracyjnych – nieprecyzyjność przepisów jako zagrożenie dla ochrony danych osobowych* [in:] *Personal data protection in public law*, ed. *eadem*, Warszawa 2021.

Jędrzejczak M., *Władza dyskrecjonalna organów administracji publicznej*, Warszawa 2021.

Jobin A., Ienca M., Vayena E., *The global landscape of AI ethics guidelines*, "Nature Machine Intelligence" 2019, No. 1(9).

Lubasz D., *Zasady legalności, przejrzystości i minimalizacji danych w ogólnym rozporządzeniu o ochronie danych osobowych w kontekście sztucznej inteligencji* [in:] *Prawo sztucznej inteligencji*, eds. L. Lai, M. Świerczyński, Warszawa 2020.

Lubasz D., Namysłowska M., *Zasady dotyczące przetwarzania danych osobowych a sztuczna inteligencja w kontekście europejskim* [in:] *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, eds. K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Warszawa 2019.

Lubasz D., Szkurłat A., *Relacja aktu o sztucznej inteligencji i ogólnego rozporządzenia o ochronie danych*, "Monitor Prawniczy" 2022, No. 21.

Ng G.W., Leung W.C., *Strong Artificial Intelligence and Consciousness*, "Journal of Artificial Intelligence and Consciousness" 2020, Vol. 7, No. 1.

Russell S., Norvig P., *Artificial Intelligence. A Modern Approach. Third Edition*, New Jersey 2016.

Szostek D., *To nie takie proste. System odpowiedzialności za algorytmy, w tym AI, z perspektywy prawa unijnego* [in:] *Prawo sztucznej inteligencji i nowych technologii 2*, eds. B. Fischer, A. Pązik, M. Świerczyński, Warszawa 2022.

Veale M., Zuiderveen Borgesius F., *Demystifying the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach*, "Computer Law Review International" 2021, No. 4.

## Summary

***Maria Jędrzejczak***

**Protection of Personal Data Processed in Artificial Intelligence Systems**

The text undertakes an analysis of European Union regulations on the prevention of data protection breaches in AI systems, taking into account the provisions of the General Data Protection Regulation (GDPR) and the draft AI Act. Legal guarantees for the protection of personal data processed in AI systems are sought in the general principles of the GDPR (in particular the principles of lawfulness, transparency, data minimisation and confidentiality) and the regulations on liability for data breaches. The conclusions of the analysis indicate that the implementation of the solutions contained in the current and proposed regulations may be hampered by the autonomy of some AI systems.

**Keywords:** artificial intelligence, draft AI Act, personal data protection.

## Streszczenie

*Maria Jędrzejczak*

**Ochrona danych osobowych przetwarzanych przez systemy sztucznej inteligencji**

W tekście podjęto analizę regulacji unijnych dotyczących przeciwdziałania naruszeniom ochrony danych osobowych w systemach AI, z uwzględnieniem przepisów RODO oraz projektu AI Act. Gwarancji prawnych dla ochrony danych osobowych przetwarzanych w systemach AI poszukuje się w zasadach ogólnych RODO (w szczególności w zasadzie legalności, przejrzystości, minimalizacji danych oraz poufności), a także w regulacjach dotyczących odpowiedzialności za naruszenia danych. Wnioski z przeprowadzonej analizy wskazują, że realizacja rozwiązań zawartych w obecnych i projektowanych regulacjach prawnych może być utrudniona z uwagi na autonomiczność niektórych systemów AI.

**Słowa kluczowe:** sztuczna inteligencja, projekt aktu w sprawie sztucznej inteligencji, ochrona danych osobowych.