PWPM 2023, Vol. XXI
PROBLEMY WSPÓŁCZESNEGO PRAWA MIĘDZYNARODOWEGO, EUROPEJSKIEGO I PORÓWNAWCZEGO
REVIEW OF INTERNATIONAL, EUROPEAN AND COMPARATIVE LAW
ISSN 1730-4504

ARTYKUŁY / ARTICLES

DOI: 10.26106/159s-q838

Protection of Personal Data in Artificial Intelligence Driven Applications

Daria Rutecka
Schoenherr Attorneys at Law, Nicolaus Copernicus University
https://orcid.org/0000-0003-3469-449; e-mail: ruteckadaria@gmail.com

1. Introduction

"Alexa, are you compliant with data privacy provisions?" Presumably, not every (if any) AI-driven application user asks this very question before downloading and installing an AI-based application on their device of choice. According to general statistics published by IDAP Group, software development company, as many as 97% of mobile users are already using AI-powered voice assistants.[1] On the other hand, experts believe that the upcoming years will bring the rise of personalized healthcare (also driven by Artificial Intelligence)[2] – this will include not only software used by professionals (embedded in medical devices), but also mobile applications freely downloadable by users. The flow and scale of personal data use is increasing with each created application and logged user. Whereas such advancement should definitely be seen as a positive development, both companies creating mobile applications, as well as users thereof must be aware of how personal data should be processed in order for the application in question to be not only efficient but also legally compliant. Undoubtedly, the correlation between personal data and AI may be summarized as follows: "[o]n the one hand,

[1] https://idapgroup.com/machine-learning/, access date: 26.10.2023.
[2] https://venturebeat.com/ai/6-healthcare-ai-predictions-for-2023/, access date: 26.10.2023.

personal data may contribute to the data sets used to train machine learning systems, namely, to build their algorithmic models. On the other hand, such models can be applied to personal data, to make inferences concerning particular individuals."[3] This article contributes to a better understanding of topical issues regarding personal data protection which are often overlooked in the fast-paced world of online applications. The methodology used is based on the intensified inspections carried out with respect of entities processing personal data through mobile applications and combines the explanation of basic rules on data processing and practical analysis and research on potential means by which the said rules could be respected.

2. AI models and approaches to machine learning

The interconnectedness between AI and data protection (that is, relevant legal provisions, with the GDPR out front) must be preceded by a short analysis of main machine learning models. Machine learning can be defined as "technology that allows system to learn directly from examples, data and experience."[4] Machine learning (together with its more sophisticated subfields such as deep learning) is currently the most popular type of AI element. The difference between regular computer programming and machine learning is that the latter allows the computer to solve problems going beyond human knowledge. That is thanks to their ability to gain their "own" knowledge through extracting patterns from raw data. Machine learning methods for conditional data generation base on building a mapping from source conditional data X to target data Y.[5] What is especially important from the legal point of view is the fact that machine learning algorithms are trained using different techniques: supervised learning, unsupervised learning, and reinforcement learning.

In supervised learning the machine is given labelled data for algorithm training in order to predict the outcome. Programmers simply provide the machine with examples of correct answers to a given question and case, thanks to which the machine is learning how to answer in a similar way when presented with a new

[3] European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 641.530 – June 2020, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, p. 1.

[4] C. Morgan (ed.), *Responsible AI, A Global Policy Framework*, "International Technology Law Association USA" 2019, p. 20.

[5] X. Tan, T. Qin, J. Bian, T.-Y. Liu, Y. Bengio, *Regeneration Learning: A Learning Paradigm for Data Generation*; Microsoft Research Mila & University of Montreal, January 2023, https://arxiv.org/abs/2301.08846, access date: 26.10.2023, p. 2.

case. In this kind of learning, the machine learns through "supervision". Examples of supervised learning include systems used for picture recognition (every photo is tagged with a specific name, e.g. of an animal), systems used for disease recognition (patients' symptoms and relevant diagnosis are linked to a given pathology) or systems used for translation (where excerpts of texts in source language X are linked to translations in target language Y).[6] Getting back to the example of a medical device or a medical application, machines trained with supervised learning methods can detect a specific anomaly only on the basis of thousands of photos or radiographies previously described by doctors as regular or abnormal. It is therefore easy to imagine what kind of sensitive data can potentially be processed by machines even through this small example itself.

Unsupervised learning bases on unlabeled data, which means that only the data itself (not labeled as correct or incorrect answer) is given to a machine. Thanks to that, machines learn how to identify patterns. However, lack of any external (human) instructions given makes this kind of training not the safest choice for systems processing personal data to a great scale (or at all). However, unsupervised training usually proves useful in cases where it is necessary to create clusters of data with similar characteristics.[7] As explained by the International Business Machines Corporation (IBM), algorithms on which unsupervised training was used, discover hidden patterns or data groupings without the need for human intervention. They are able to discover similarities and differences in information.[8] Nevertheless, one of main challenges related to the use of such algorithms is the lack of transparency into the basis on which data was clustered, which makes them potentially dangerous in case of personal data processing.

Following the words of Noel E Sharkey, authors of *Responsible AI. A global policy framework* also admit that the reinforcement learning (training) is "essentially the application of Pavlov's dog theory to AI."[9] In reinforcement training the machine is also trained by the use of examples. However, the system is in a way "rewarded" for every improvement it makes which brings it towards the accomplishment of a goal. It can be said that the system learns through the outcomes of its own actions (i.e., whether it receives a reward or a penalty).

Given the above, it is not surprising that the supervised training is still the most common and popular method for algorithm training as it gives the best certainty of the data used and outcomes (to be) achieved using AI. All of the

6 European Parliamentary Research Service, *The impact of the General Data Protection Regulation...*, p. 10.

7 C. Morgan (ed.), *Responsible AI...*, p. 22.

8 https://www.ibm.com/topics/unsupervised-learning, access date: 26.10.2023.

9 C. Morgan (ed.), *Responsible AI...*, p. 22.

above explanations should serve as a starting point in grasping the idea of, often misunderstood, rules of mobile applications.[10]

3. The use of AI towards profiling, decision-making and the fate of individuals

Content profiling, automated decision-making and personalized advertisements are possible thanks to the elements of AI. The abovementioned supervised training, widely used in app creating may contain traces of human judgements (concerning ethnicity, gender, nationality or even political views) which could have been used for machine training. According to Article 22 of the GDPR data subjects (individuals) have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. The above provides a right not to be subject to a completely automated decisions having any potential impact on the data subject. As a rule, automated decision making is prohibited.

Article 22 paragraph 2 of the GDPR contains a closed catalogue of exceptions which allow automated decision-making. These include: (i) situations where it is necessary for entering into, or performance of, a contract between the data subject and a data controller, (ii) cases where such use is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, (iii) situations where the automated processing is based on the data subject's explicit consent. When relying on exemptions (i) and (iii) the data controller must implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. Additionally, automated decisions should not be based on "special" categories of personal data (special categories include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation) unless additional requirements are met. Those requirements include relying on data subject's clear consent or on the exception of processing being necessary for reasons of substantial public interest, based on Union

[10] C. Durt, *Artificial Intelligence and Its Integration into the Human Lifeworld* [in:] S. Voeneky, P. Kellmeyer, O. Mueller, W. Burgard, *The Cambridge Handbook of Responsible Artificial Intelligence, Interdisciplinary perspectives*, Cambridge 2022, p. 67.

or Member State law (which, in turn, must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject). The last requirement involves the existence of suitable measures to safeguard the data subject's rights and freedoms, as well as legitimate interests.

In their joint opinion 5/2021 issued on 18 June 2021 the European Data Protection Board and the European Data Protection Supervisor strongly call for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces (faces, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioral signals) in any context.[11] Therefore, even consent given by relevant data subjects could be potentially challenged in this scenario.

When assessing the (potential) impact AI may have on individuals with respect to profiling and automated decision-making processes, one must inevitably take into account the contents of GDPR's recitals, which still prove useful, even after five years of GDPR's applicability. Recital 71 to the GDPR, as main examples of automated decisions which significantly affect or have legal impact on an individual presents "automatic refusal of an online credit application or e-recruiting practices without any human intervention."[12] Other examples are health-related or education applications, as well as analyzing or predicting aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.[13] Considering even just the increasing number of AI-driven recruitment applications, the actual impact of a decision taken really by AI on an individual becomes more apparent. The "forbidden" automated decisions, as mentioned in Article 22 paragraph 1 of the GDPR cover a lot of possible AI applications. The use of AI algorithms is increasing especially in areas such as recruitment, access to insurance, health services, social security. This is even more true considering large scale systems used on thousands or even millions of users. Therefore, "it is more likely that a decision will be based 'solely' on automated processing."[14]

---

11 EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, p. 11.

12 Recital 71 to the GDPR.

13 M. Jankowska, M. Pawełczyk, M. Sakowska-Baryła, *Sztuczna inteligencja i wybrane aspekty cyfrowej transformacji w systemie medycznym* [in:] B. Fischer, A. Pązik, M. Świerczyński, *Prawo sztucznej inteligencji i nowych technologii 2*, Warsaw 2022, p. 223.

14 European Parliamentary Research Service, *The impact of the General Data Protection Regulation...*, p. 60.

Using AI algorithms in decisions impacting individuals requires a set of relevant safeguard measures safeguarding the data subject's rights and freedoms and legitimate interests (at least the right to obtain human intervention on the part of the controller), to express his or her point of view and to contest the decision. The catalogue of actions required from the controllers is a broad one. The "controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organizational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimized, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect."[15]

The input data used for both training the algorithms and, subsequently, used in each specific case and regarding a specific individual cannot be taken out of context, irrelevant or inaccurate. The Article 29 Working Party emphasized that such data cannot violate the reasonable expectations of the data subjects. When analyzing the scope and method of data gathering, one cannot ignore the mediums on which data is usually gathered: smartphones, smartwatches, computers etc. Every information, including sensitive health-related details or information about even smallest daily transaction recorded on banking application is saved and processed further. Thus, application users have become easy to track, influence and, as a result and to some extent, control.[16] Furthermore, when considering the fate of data subjects in the era of such tremendous technological development, not acknowledging the importance of potential data transfers would be a negligence. Mobile applications, used for example for navigating vehicles or even to operate smart fridges, include a vast amount of data which is further transmitted not only to the manufacturer of the given product in which the app is embedded but also to other service providers. Each of the data controllers and processors may be placed in different country and thus, the cross-border data flows are inevitable.[17] The rules of personal data processing as mentioned below and applied in the provisions of the GDPR must be strictly observed in this respect.

---

15 Recital 71 to the GDPR.

16 L. Lai, *Some reflections on the use of tracking applications based on AI algorithms to curb the COVID-19 pandemic* [in:] L. Lai, M. Świerczyński (eds), *Legal and Technical Aspects of Artificial Intelligence*, Warsaw 2021, p. 179.

17 T. Naef, *Data Protection without Data Protectionism. The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law*, London 2023, p. 239.

4. Rules of personal data processing and trustworthy AI

On 19 February 2020 the European Commission published the White Paper on AI – A European approach to excellence and trust.[18] The White Paper sets out policy options on how to achieve the twin objective of promoting the uptake of AI and of addressing the risks associated with certain uses of such technology. Following up on that, on 21 April 2021 the European Parliament and the Council issued a proposal for the Regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts. Both the White Paper as well as the AI Act proposal were deliveries on the political commitment by President von der Leyen, who announced in her political guidelines for the 2019–2024 Commission that the Commission would put forward legislation for a coordinated European approach on the human and ethical implications of AI.[19] Similarly, both of those acts, when referring to the use of Artificial intelligence, highlight its key feature – trustworthiness. When considering the data privacy in particular, the trustworthiness of AI cannot be interpreted and viewed in isolation from basic rules of personal data processing laid down in the GDPR.

Firstly, processing of personal data should be lawful and fair, which means that data subjects must be aware that their personal data are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed (and – by whom or rather by what). The rule of lawfulness and fairness must be interpreted broadly and should override other rules of processing.[20] That is because this very rule is executed by implementing all other rules: by providing transparency, adequacy of the data processed, their relevancy and limiting such data to what is necessary for the purposes for which they are processed.[21] In addition to the above personal data should be processed in a manner ensuring appropriate security and confidentiality of the personal data, including for preventing unauthorized access to or use of personal data and the equipment used for the processing. Moreover, data controllers should be able to prove that they have complied with all of those rules.[22] Lawfulness of data processing is nothing else but applying the conditions set out in Article 6 of the GDPR: consent, necessity for the performance of a contract

[18] European Commission, White Paper on Artificial Intelligence – A European approach to excellence and trust, COM (2020) 65 final.

[19] Proposal for a Regulation of European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Brussels, 21.04.2021, COM (2021) 206 final, 2021/0106 (COD).

[20] K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, Warsaw 2019, p. 206.

[21] Recital 39 to the GDPR.

[22] *Ibidem*.

to which the data subject is a party (or taking steps at the request of the data subject prior to entering into a contract), necessity for compliance with a legal obligation to which the controller is subject, necessity for protection of the vital interests of the data subject or of another natural person, necessity for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, necessity for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Fairness and transparency, on the other hand, refer to the mere fact that a data subject is well informed about processing of their data (informational fairness) and the abovementioned contend of automated interference or a decision (substantive fairness).[23] Taking all of the above into account, when designing solutions based on Artificial Intelligence and using them in applications having a daily impact on data subjects' lives, the creators must introduce relevant measures which would prevent discriminatory treatment or solutions basing on inadequate or inaccurate data. In short, application users, being data subjects, must reasonably expect the purpose and scope of their data being processed. All communications regarding processing and usage of personal data must be easily accessible and understandable to date subjects.

Another rule of personal data processing, especially crucial in case of data processed using AI technologies, is the rule of processing purpose limitation. Personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes."[24] This rule is of particular importance in case of machine learning as it prevents personal data from being collected for future purposes which are unspecified and unknown to the data subject. Only well and properly informed data subject is capable of fully exercising their rights and acting within their informational autonomy letting them decide, e.g., which entities may process their personal data. The European Parliamentary Research Service duly emphasizes that there is a tension between the use of Ai and big data technologies and the requirement of purpose limitation. The gist of such technologies is the reuse of data for new purposes. As one of many examples one may indicate personal data collected for contract management which could

[23] European Parliamentary Research Service, *The impact of the General Data Protection Regulation...*, pp. 44–45.

[24] Article 5 item b of the GDPR.

potentially be processed for advertisement targeting and learning consumers' preferences in the future[25]. On 7 February 2023 Microsoft launched a new, AI-powered Bing search engine. Thanks to the use of AI, the new search engine provides "[a]n improved version of the familiar search experience, providing more relevant results for simple things like sports scores, stock prices and weather, along with a new sidebar that shows more comprehensive answers [...]."[26] The innovations introduced would not be possible without repurposing the use of data gathered. The repurposing of personal data, in order to be permitted, needs to be legitimate. The Article 29 Working Party indicated that the criteria to be taken into account when assessing if the new purpose is compatible with previous one include: the distance between the old and new purpose, the compliance of the new purpose with reasonable expectations of the data subject, the nature of the data and the impact of the further processing on the data subjects, the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects[27]. In January 2021 the Spanish Data Protection Agency issued "Audit requirements for Personal Data Processing Activities involving AI" where it proposed a few general solutions ("controls") which may help determine whether the repurposing is legitimate. First of all, the intended usage and purpose of the given AI-based component must be documented with respect to both its quality and quantity. What is more, the goal of such component, its usage, as well as relationship between the goal and usage and technical conditions guaranteeing lawfulness must also be clearly described. Users and potential users of the AI-driven application and component must be defined upfront. Any secondary uses of data collected previously must be documented and have legal grounds.[28]

Data gathered for the use of AI-powered mechanisms, just like personal data in any other case, must be minimized and limited (likewise, data retention also needs to be restricted and minimized). Article 5 of the GDPR clearly states that personal data (gathered for any purpose and by any means) must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The question arises: how to minimize data gathered e.g. for the purpose of machine learning? To demonstrate compliance with this the GDPR, the controller should

[25] European Parliamentary Research Service, *The impact of the General Data Protection Regulation...*, p. 45.

[26] https://blogs.microsoft.com/blog/2023/02/07/reinventing-search-with-a-new-ai-powered-microsoft-bing-and-edge-your-copilot-for-the-web/, access date: 26.10.2023.

[27] Article 29 Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013, pp. 23–27.

[28] Spanish Data Protection Agency (Agencia Española de Protección de Datos), *Audit requirements for Personal Data Processing Activities involving AI*, https://www.aepd.es/documento/requisitos-auditorias-tratamientos-incluyan-ia-en.pdf, access date: 26.10.2023, p. 15.

adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Once again, just like in case of the purpose limitation, similarly in case of the rule of data minimization there is a mismatch of goals to be achieved between the rule of data minimization and the very idea of big data and AI-involving data analytics. This tension and potential issue may be solved by regular audits of AI-driven mechanisms (in terms of what data is still needed for the development thereof). Additionally, data minimization must be combined with the rule of proportionality allowing for the extra data to be collected in case it may prove useful.

Finally, personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures. When it comes to AI-based applications, the above should be achieved by the risk-based approach and the idea of data protection by design and by default. Privacy by design means that the issue of data privacy and safety must be considered already when designing the application, whereas privacy by default means "privacy" must be included in default settings of the app. This, in turn, means that before choosing a given technical and organizational measure and relevant safeguards, data controllers should perform risk assessment activities. After all, it is obvious that health-related data will require different safeguards and protection than data on music preferences.

5. Final remarks

Artificial Intelligence and its extensive use in applications used every day by millions of users is not incompatible with the GDPR as a rule. When applying given technology in personal data processing activities, data controllers and app creators must always bear in mind general rules and standards set out in the GDPR and related acts in each jurisdiction. All of the above remarks remain accurate regardless of the type of mobile application involved: whether it is a health app or banking application, unbiased treatment must be treated as an essential.[29] It is worth mentioning here that on 23 October 2023 the European Data Protection Supervisor issued another opinion on the Artificial Intelligence Act.[30] Interestingly, the European Data

[29] L. Dionysopoulos, *Historic Overview and Future Outlook of Blockchain Interoperability* [in:] J. Soldatos, D. Kyriazis, *Big Data and Artificial Intelligence in Digital Finance, Increasing Personalization and Trust in Digital Finance using Big Data and AI*, London 2022, p. 113.

[30] https://edps.europa.eu/press-publications/press-news/press-releases/2023/edps-final-recommendations-ai-act_en, access date: 26.10.2023.

Protection Supervisor considers that it is crucial that individuals affected by the use of AI systems are provided with the right to lodge a complaint before a competent authority in case providers and users of AI systems infringe on the relevant acts. Artificial Intelligence practitioners must, therefore ensure that their systems comply with both the Artificial Intelligence Act (and other legislation issued after its publication) and the data protection legislation.[31] The key to compliance with the GDPR is, among others, understanding the aim of application as well as business model of the service rendered through the app.[32] The latter can include mobile app for an on-line store, intermediation service (e.g., Uber), smart home application, social media, health and medical applications. In light of both growing development of innovations and quite restrictive potential fines which could be imposed on data controllers in case of breach, the safest and most efficient way of ensuring compliance are regular security tests and audits. Additionally and finally, data controllers must always be aware of what happens to the data they control, even (and especially) if such data has been forwarded to AI-based system.

Abstract

In a fast-paced society the use of mobile applications increased tremendously. Mobile applications are convenient and could potentially contribute to making everyday life easier. The article points out key issues which may occur in case of processing of personal data by Artificial Intelligence based applications and describes key rules which must be considered when processing personal data.

Key words: AI, Artificial Intelligence, mobile applications, apps, personal data, data privacy, data processing

Streszczenie

W szybko rozwijającym się społeczeństwie znacznie wzrósł poziom korzystania z aplikacji mobilnych. Aplikacje te są wygodne i mogą przyczyniać się do ułatwienia codziennego życia. Artykuł wskazuje kluczowe problemy, które mogą wystąpić w przypadku przetwarzania danych osobowych przez aplikacje oparte na sztucznej inteligencji, i opisuje najważniejsze zasady, które należy wziąć pod uwagę przy przetwarzaniu danych osobowych.

Słowa kluczowe: sztuczna inteligencja, aplikacje mobilne, aplikacje, dane osobowe, prywatność danych, przetwarzanie danych

[31] European Data Protection Supervisor, Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments, 23 October 2023, https://edps.europa.eu/system/files/2023-10/2023-0137_d3269_opinion_en.pdf, access date: 26.10.2023.

[32] M. Gumularz, *Ochrona danych osobowych w aplikacjach mobilnych*, „ABI expert", April–June 2022, no. 2 (23).