# AI-BASED PERSONALIZATION AND PRIVACY PROTECTION: CAN CURRENT LAWS EFFICIENTLY PROTECT ONLINE USERS?

Alžběta Solarczyk Krausová*

***Abstract:*** *AI-based personalization is a technology that uses vast amounts of personal data to tailor experience for online user and provide them with information they require. On one hand, it can make it easier for users to receive relevant information, on the other hand it can also manipulate their decision-making process, lower their personal autonomy, as well as intrude in their privacy. The aim of this paper is to answer the question whether the current EU laws efficiently protect personal autonomy and the rights to privacy and data protection of online users in the context of AI-based personalization. The paper explores the notion of "efficient protection" and the specific legal challenges that AI-based personalization poses for the protection of personal autonomy, privacy, and data protection.*

***Keywords:*** *artificial intelligence, personalization, personal autonomy, right to self-determination, GDPR, recommender systems, AI Act, consent*

## INTRODUCTION

Most of us are spending hours a day in an online environment. Our minds constantly engage with digital content, consume texts, pictures, and videos, and communicate via social media platforms. We receive information about our peers, information about what is going on in the world, and advertisements about products or services we can buy. The online world is providing us with way too much information. This results in information overload and a short attention span in people using the modern technologies. Online platforms came with a technology solution to this problem – personalization.

Personalization is a technique how to show online users content that is the most relevant for them. It is based on algorithms utilizing information about users to analyze their behavior and infer their preferences. Former personalization algorithms were mostly static and had quite limited abilities on how to tailor the content to users. However, with the continuous progress and growing use of artificial intelligence (AI), as well as rapidly growing datasets about online user behavior, personalization becomes much more efficient. AI is currently able to tailor online experience for each user individually and, thus, guide their decision-making more efficiently. And it is this feature that raises a number of questions related to protection of online users.

Decision-making is the fundamental characteristics of personal freedom and personal autonomy. Personalization replaces decision-making process of individuals and does so by getting to know them through extensive collection and processing of personal data and intruding their privacy. Given the factual use of this technology and a significant impact of it on rights of users, it is necessary to question whether they have any means for

* Mgr. Alžběta Solarczyk Krausová, Ph.D., LL.M., Institute of State and Law of the Czech Academy of Sciences, Prague, Czech Republic. E-mail: alzbeta.krausova@ilaw.cas.cz. ORCID 0000-0002-1640-9594.
This paper was supported by the Technology Agency of the Czech Republic under the grant No. TL03000152 "Artificial Intelligence, Media, and Law."

protecting themselves from potentially negative consequences or even misuse of personalization. There are of course existing legal provisions ensuring protection of fundamental human rights, privacy and data. However, it is questionable whether they can provide factual guarantees and what limitations to exercising own rights may exist.

Therefore, the aim of this paper is to answer the question whether the current EU laws efficiently protect personal autonomy and the rights to privacy and data protection of online users in the context of AI-based personalization. The paper explores the notion of "efficient protection" and the specific legal challenges that AI-based personalization poses for the protection of personal autonomy, privacy, and data protection.

## I. AI-BASED PERSONALIZATION IN THE LEGAL CONTEXT

AI-based personalization is a technology that is not regulated by a sole legal instrument. Depending on the context or usage, personalization can fall under different legal regimes.

As stated above, personalization can be understood as an algorithm-based technology aiming at providing individualized services and online experience to users. It collects data about users, infers information about their patterns of behavior and personal preferences. The algorithms then provides services and experience to user as they – algorithms – decide. The logic behind their decision-making is not generally known and if yes, then definitely not to the granular level. By this I mean that users will not know how much are their interests taken into account when an algorithm decides. Or if their interests are taken into account at all. Algorithms are designed by technology providers presumably mostly for their own benefit. In fact, they control users' behavior by limiting their control over an online environment and forcing them to accept what an algorithm deems fit for them. In order to have a complex view, we need to distinguish personalization from another term – customization. Customization means that it is the users how benevolently set up their preferences when directly asked by a technology provider (including a content provider). Algorithms then do not infer users' preferences from their behavior but from their own choice. Moreover, customization does not generally entail such a broad personal data processing as personalization.

AI-based personalization can be based on various techniques and serve more purposes. Given the context and technological nature of a particular use of personalization, there can be at least three applicable legal instruments:

- General Data Protection Regulation (GDPR):[1] personalization typically falls under the regime of the GDPR given the vast amount of personal data processing. Personalization itself typically falls under the practice of automated individual decision-making and profiling (Art. 22 GDPR). Profiling in this sense means "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person" and personal preferences are explicitly mentioned in this regard (Art. 4(4) GDPR).

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

- Digital Services Act (DSA):[2] personalization can fall under the definition of so called recommender system. This is "a fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service or prioritise that information, including as a result of a search initiated by the recipient of the service or otherwise determining the relative order or prominence of information displayed". The DSA sets out specific transparency obligations for providers of online platforms that aim to protect personal autonomy and indirectly also privacy (Art. 27 DSA).
- AI Act (AIA):[3] In case a particular use of personalization utilizes an AI system, it falls under this regulation. AI system is defined as "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments" (Art. 3(1) AIA).

In the following chapter, these legal instruments will be assessed from the perspective of providing "efficient protection" to users. This term refers to the ability of a particular legal provision (or a piece of legislation) to really protect a person in a particular situation, i.e. allow them to exercise their rights fully, successfully request compensation, or prevent others from violating guaranteed rights). In the specific case of personalization, it includes the ability to understand the functioning of personalization systems, to make informed choices about data processing, and to challenge or opt out of automated decision-making where appropriate. The adequacy of existing EU legislation is therefore assessed not only in terms of legal requirements, but in their capacity to safeguard individual autonomy and privacy in real, technologically complex conditions.

## II. LEGAL INSTRUMENTS FOR PROTECTION OF PERSONAL AUTONOMY AND PRIVACY

In the context of modern technologies and especially AI-based personalization, the law is often criticized as inefficient. Some authors consider personalized algorithmic decision-making as inherently threatening personal autonomy and resulting ethical and legal challenges cannot be fully resolved there, not even by technological solutions.[4] Others point out to challenges in the area of privacy, informed consent, and algorithmic bias. They argue that current legal frameworks are insufficient and require adaptive

[2] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)

[3] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)

[4] LU, Wencheng. Inevitable challenges of autonomy: ethical concerns in personalized algorithmic decision-making. *Humanities and Social Sciences Communications*. Palgrave, 2024, Vol. 11, No. 1, p. 1–9. ISSN 2662-9992. DOI: 10.1057/s41599-024-03864-y

governance, international harmonization, and integrated technical-ethical safeguards.[5] Opacity of algorithms is considered as one of the key issues in eroding personal autonomy.[6]

The General Data Protection Regulation (GDPR), the Digital Services Act (DSA), and the Artificial Intelligence Act (AI Act) all offer substantive and procedural guarantees that must be examined in light of the fundamental value of personal autonomy in order to determine whether the EU's current legal tools adequately shield users from the detrimental effects of AI-based personalization.

As a legal and philosophical concept, personal autonomy refers to people's capacity to make free, informed decisions without interference or coercion. Whether people maintain control over their decisions or if this autonomy is gradually undermined by opaque and ubiquitous algorithmic systems is the main question in the digital world, where AI-based personalization works by influencing user behavior through targeted content.

As the cornerstone of data protection in the EU, the GDPR offers important protections to guarantee user control, transparency, and data minimization. Particularly pertinent is Article 22 of the GDPR, which governs automated personal decision-making, including profiling. This clause gives people the right to refuse to be subject to a decision that is made purely on the basis of automated processing if that decision has significant or legal ramifications. There are, however, some exceptions, such as when processing is required to fulfill a contract, permitted by law, or supported by express consent. Although this right is a legal protection, its applicability is questionable. Because of information asymmetry and the complexity of AI systems, the requirement of explicit consent may not always be met in a meaningful way. Moreover, users may be unaware that personalization constitutes automated decision-making, thereby limiting their ability to invoke their rights effectively.

Through Articles 13 to 15, which require that data controllers notify users of the existence of automated decision-making and provide meaningful information about the logic involved, the GDPR further emphasizes accountability and transparency. However, this clause is frequently ineffective in practice due to both the ambiguity surrounding what "meaningful information" is and the technical inaccessibility of algorithmic processes. Therefore, even though the GDPR creates a strong framework in theory, there are major obstacles to its implementation in practice.

By focusing on the design and conduct of online platforms, the DSA complements the GDPR. Recommender systems are subject to transparency requirements under Article 27, which require that platforms notify users of the primary parameters of these systems and offer ways for them to be changed. Enhancing user agency and reducing covert algorithmic influence are the goals of this step. The DSA does not, however, address more serious issues with algorithmic manipulation or the psychological effects of customized content, nor does it place meaningful restrictions on the use of personalization. Its primary focus is still procedural.

---

[5] MIRISHLI, Shahmar. Ethical Implications of AI in Data Collection: Balancing Innovation with Privacy. *ANCIENT LAND*. 2024, Vol. 6, No. 8, p. 40–55. ISSN 27066185, 27094197. DOI: 10.36719/2706-6185/38/40-55.

[6] VAASSEN, Bram. AI, Opacity, and Personal Autonomy. *Philosophy & Technology*. 2022, Vol. 35, No. 4, p. 88. ISSN 2210-5433, 2210-5441. DOI: 10.1007/s13347-022-00577-5.

A risk-based regulatory framework is introduced by the AI Act, though it is not yet fully operative. Strict requirements apply to systems that pose significant risks to fundamental rights, such as those that impact access to essential services, work opportunities, or education. Depending on their use, personalization AI systems may be included in this category. By requiring accountability, transparency, and human oversight, the AI Act may improve safeguards against personalization that reduces autonomy. However, its wide definitions and dependence on providers' risk assessments could lead to uneven enforcement and classification.

The three tools provide overlapping protections from a systemic standpoint. However, there are still large gaps. The absence of operational coherence and integration between them is the most significant constraint. Users may find their rights less practically enforceable as a result of having to navigate several frameworks with disparate terminologies, processes, and thresholds. Furthermore, even though transparency is important, it is insufficient without significant control over how personalization technologies function and influence user behavior.

In conclusion, intellectual ambiguity, procedural complexity, and enforcement issues limit the efficacy of the GDPR, DSA, and the AI Act, even though they all help to safeguard individual autonomy in the context of AI-based personalization. Legal tools must advance to provide users with real control mechanisms in addition to information, backed by oversight and technological accountability, if protection is to be genuinely effective. Without these improvements, legal guarantees run the risk of continuing to be primarily formal and having little practical ability to protect individual liberty.

## CONCLUSION

Personalization is a really powerful technological tool which the legal system attempts to specifically regulate. Despite its obvious benefits in delivering individually relevant content, personalization also has a huge potential in manipulating people. It would be naïve to think that such algorithms are used primarily for users' benefit. It is probably more appropriate to claim that deployers of personalization algorithms are searching for win-win solutions and protect also their own business interests. Law is a systems that strives to find balance among competing interests of various subjects. Therefore, it can never provide an ideal solution that would benefit everyone as it is based on the presumption that people's interest are often in conflict. The presented legal instruments are also a compromise attempting to protect users' autonomy and privacy on one side and freedom to do business on the other side. Their efficiency is limited especially because of the complexity of the problem. Law does create a framework for technology providers that requires them to adhere to certain standards and algorithmic governance. Law does also provide efficient tools how to protect oneself – be it in the form of general protection of fundamental human rights, in specific provisions that guarantee explainability and the right to choose a technology solution, give or withdraw consent, require explanations, switch off personalization, or sue a technology provider. However, it is the limited capacity of users to protect themselves that causes the real issues. Law can provide a framework and tools. Unfortunately, in the new and increasingly complex technological world, the traditional approaches of exercising own rights cease to work. We need to change

our perspective and come up with legal and most importantly societal solutions that will react on the fact that people are giving up on their personal autonomy and privacy by themselves. Under such conditions, law cannot protect users against their own will. The Roman principle *"vigilantibus iura*" has in this sense universal validity.

Given the benefits of personalization in suppressing information overload and delivering relevant content and preferred experience, it is advisable to find a solution that would shift control back to users while keeping the mentioned benefits. The most appropriate solution is to make it more beneficial for technology providers to switch to customization when user would be provided with much more choice. Research, however, shows, that such mechanisms for exercising own choice need to be skillfully designed not to paralyze users again with excessive amount of questions, repeated asking for setting up preferences, etc. Such practice could be again understood as manipulative and aiming at exhausting the biologically limited capacity of decision-making by humans.