PERSONALIZATION BEYOND CONVENIENCE: NAVIGATING PRIVACY AND PERSONAL DATA PROTECTION ISSUES

Kristýna Akil*

Abstract: *Personalization is widely promoted as a mechanism for enhancing consumer convenience and relevance. Yet, its underlying data practices increasingly raise concerns about individual autonomy and privacy. This article examines how personalization systems operate across personal, non-personal, and inferred data. It argues that these forms of data processing can interfere with informational, decisional, and psychological dimensions of privacy. Building on analysis of European privacy and data protection law and judicial practice, this article highlights conceptual tensions between personalization and the GDPR, particularly regarding the legal status and oversight of inferred and non-personal data. It demonstrates that current data protection safeguards insufficiently address the privacy risks stemming from personalization techniques that influence users' choices, perceptions, and behaviour without relying solely on personal data processing. With regards to possible harms, this article also analyses personalization as potential automated decision-making under Article 22 GDPR. The article concludes that understanding and mitigating the privacy challenges of personalization requires moving beyond legal definitions of personal data to consider the broader ways in which digital systems shape autonomy and decision-making.*

Keywords: *Personalization, personal data, privacy, profiling, automated decision-making*

INTRODUCTION

Personalisation is increasingly becoming a defining feature of the digital environment. For many consumers, it represents a convenient service that allows them to obtain more relevant search results, interesting content, and potentially attractive advertising. To provide this experience, businesses employ tracking technologies that continuously monitor various aspects of individuals' lives, analysing their online activity, influencing their experience and even shaping their future behaviour.

Although personalization is not a new phenomenon,[1] the law has only recently started gradually dealing with problems which personalization might be bringing. The European Union has lately been active in regulating the digital environment, personalization included. The Digital Services Act "DSA" draws attention in particular to transparency and establishes special measures for advertisements in Article 26 and 28 and for recommendation systems in Article 27.[2] Similarly, the update of the Consumer Rights Directive[3] poses an obligation on traders in Article 6/1/e to inform consumers about any

* Mgr. Kristýna Akil, Researcher at the Institute of Law and Technology at Faculty of Law, Masaryk University, Brno, Czech Republic; Lawyer at the Data Protection Office at Rector's Office, Masaryk University, Brno, Czech Republic. E-mail: kristyna.akil@law.muni.cz. ORCID: https://orcid.org/0009-0006-7208-2107. This article was written as part of the author's research project PANOPTICON – Personalization and the need of privacy: transcending information challenges, project code MUNI/A/1781/2024, supported by Masaryk University within specific research – support for student projects in 2025.

[1] Cf. KANIEWSKA-SĘBA, Aleksandra. Negative effects of personalization in direct marketing. *International Journal of Arts & Sciences*. 2014, Vol. 7, No. 2, pp. 89–98.

[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).

[3] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on Consumer Rights.

occurrence of personalized pricing based on automated decision-making. A similar provision has been adopted within the current proposal for a new Consumer Credit Directive in Article 13[4] and some authors derive the same obligation from Article 7/1 of the Unfair Commercial Practices Directive (UCPD).[5]

Among scholars, there are ongoing discussions about the effects of personalization and the possible need for regulation.[6] Nonetheless, to the best of the author's knowledge, no existing legal literature addresses the complexity and extent of the possible harm to different privacy spheres which are concerned and the interconnection with the data protection questions. Although privacy concerns are frequently noted, the detailed mechanisms through which personalization interferes with different aspects of privacy remain unexplored. Furthermore, most discussions focus primarily on personal data processing under the GDPR, while the possible privacy implications of non-personal, inferred or anonymised data, which can still influence consumer autonomy and behaviour, receive considerably less attention.

This article mainly addresses the question of how personalization impacts privacy, specifically which dimensions of user's privacy are affected by digital personalization practices, beyond the processing of personal data, how the stages of personalization potentially compromise these privacy dimensions, and finally, if personalization can be considered a form of automated decision-making under Article 22 GDPR, considering its impact on person's fundamental right to privacy.

In this article, I first define personalization and introduce its possible forms. I then break down personalization into detailed steps, revealing the individual parts of this complex process. This is a key step to examine how personalization operates with data and information about consumers in order to further analyse how the privacy is interfered with. The article then proceeds to privacy regulation, analysing the broad concept of privacy both from a theoretical and a legal point of view, highlighting the overlap of privacy and data protection. The crucial, last part of this work lies in analysing the privacy issues of personalization and connecting them to the specific parts of the personalization process. Within the personal data protection framework, special emphasis is placed on automated decision-making and, more specifically, the possibility to qualify the process of personalization as automated decision-making under Article 22 GDPR.

I. PERSONALIZATION – AN EMPOWERING TOOL, OR RELENTLESS WATCHER?

Personalisation is a business strategy in the digital environment which aims to offer recipients the most relevant, personalised online content, including adverts or prices. Tailoring offers to individual consumers is made possible by technologies tracking their preferences and by subsequent data analysis of the data collected. The imple-

[4] Proposal for a Directive of the European Parliament and of the Council on consumer credits.

[5] ROTT, Peter et al. Personalized pricing. *Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies*. 2022, p. 7 In: *European Parliament* [online]. [2024-11-12]. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/734008/IPOL_STU(2022)734008_EN.pdf.

[6] Cf. BASTIAN, Mariella. *News personalization for peace: how algorithmic recommendations can impact conflict coverage.*

mentation of personalisation both on websites and smart devices make surveillance broad and ubiquitous, increasing its reach into diverse activities of people's daily lives. The companies use technologies such as cookies, tracking pixels or others to detect behavioural patterns while the user is interacting with ads, articles, videos or social media posts. This data may include a wide range of types of information, including demographic data such as age, gender or location; behavioural (technical) data such as the pages visited by the user, the time spent on those pages and the types of content the user consumes; and interest data, which is derived from user preferences.[7] Through further data analysis, more information can be revealed about an individual, such as his or her political affiliation, religious beliefs, sexual identity, race and ethnicity, education level, income group, shopping habits and physical and mental health. Advanced algorithms allow marketers to analyse the information collected and create detailed profiles of users, which are then used as the basis for displaying targeted content.

Personalisation, while often framed as a tool for convenience and efficiency, can give rise to a range of significant risks. One of the most frequently discussed concerns is discrimination,[8] which occurs when algorithmic decision-making systematically disadvantages certain groups of users by displaying them different offers than to others. For example, profiling based on behavioural or demographic data may reinforce assumed social biases and exclude particular individuals from economic opportunities,[9] or lead to unequal access to services or information,[10] which can also interfere with right to information. Such algorithmic discrimination can operate subtly and unintentionally, yet its impact can be significant, especially if personalized content or offers target or exclude users based on sensitive attributes such as race, gender, age, or socioeconomic status.

Another critical consequence of personalization is possible autonomy violation, where content and recommendations are designed to influence consumer behaviour, often without the individual's explicit awareness.[11] Personalization can exploit users' cognitive biases or emotional states,[12] shaping choices in ways that may conflict with their autonomous decision-making. Relatedly, personalization can exploit user vulnerability, as algorithms may identify and target individuals in states of emotional, financial, or cognitive sensitivity, increasing the likelihood of harmful impact. Autonomy concerns

[7] SAXENA, Ashish K. Beyond the Filter Bubble: A Critical Examination of Search Personalization and Information Ecosystems. *International Journal of Intelligent Automation and Computing*. 2019, Vol. 2, No. 1, p. 55.

[8] CELIS, Elisa L. et al. Controlling Polarization in Personalization. *Proceedings of the Conference on Fairness, Accountability, and Transparency*. 2019, pp. 160–169.

[9] European Data Protection Board. *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*. 2018.

[10] BASTIAN, Mariella. *News personalization for peace: how algorithmic recommendations can impact conflict coverage,* p. 310.

[11] TOCH, Eran et al. Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems. *User Model User-Adap Inter*. 2012, Vol. 22, p. 207.

[12] Cf. GUNAWAN, Johanna – SANTOS, Cristiana – KAMARA, Irene. Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions. *Proceedings of the 2022 Symposium on Computer Science and Law. (CSLAW, 22)*. Association for Computing Machinery, 2022 New York, pp. 181–194.

are often framed around consumer manipulation[13] and some explore the impact of personalization specifically on consumer vulnerability.[14]

Additionally, personalization contributes to the formation of filter bubbles and rabbit holes,[15] in which algorithm guides users to narrow perspectives, reinforcing existing beliefs and making alternative information less accessible without extra effort from the user. Collectively, these effects demonstrate that personalization is not merely a technical or commercial practice, but a phenomenon with strong implications for autonomy, fairness, and the broader societal and informational environment. In this article, I will further focus on privacy implications of personalization,[16] encompassing autonomy and control over information about oneself.

Taken together, these harms show that personalization relies heavily on the use of personal data and on forms of surveillance that can interfere with individuals' autonomy. Since autonomy itself is a core dimension of privacy, understanding these harms requires a closer look at how privacy relates to personal data protection.

II. THE CONCEPTUAL TENSION: PRIVACY VS. DATA PROTECTION

Privacy is a concept that has been difficult to define comprehensively due to its various aspects and dimensions. Over time, scholars have created several typologies to capture its complexity. Among the most frequently cited is the definition offered by Warren and Brandeis at the end of the 19th century, which frames privacy as the right to be let alone.[17] This foundational concept continues to influence modern theorists, including those who examine privacy in digital era.[18] Brandeis' and Warren's principles remain a reference point in privacy debates and for understanding privacy as a protection against unwanted interference.

Westin approaches privacy from a similar perspective, distinguishing privacy as solitude and anonymity and emphasizing an absence of interference.[19] However, contrary to right to be left alone, Westin focuses on how privacy can be maintained even in public or partially monitored spaces. His understanding of solitude refers to freedom from any intervention or surveillance, whereas anonymity, treated as a less strict component of privacy, presumes that an individual is not actively monitored or identifiable. According to Westin, a person may attain anonymity even in public settings without solitude, as

[13] MANWARING, Kayleen. Will Emerging Technologies Outpace Consumer Protection Law? The Case of Digital Consumer Manipulation. *Competition and Consumer Law Journal*. 2018, Vol. 26, No. 2, pp. 141–181.

[14] CHEN, Si et al. How does ad relevance affect consumers' attitudes toward personalized advertisements and social media platforms? The role of information co-ownership, vulnerability, and privacy cynicism. *Journal of Retailing and Consumer Services*. 2023, Vol. 73, p. 1.

[15] BASTIAN, Mariella. *News personalization for peace: how algorithmic recommendations can impact conflict coverage*, p. 316.

[16] BASTIAN, Mariella et al. *News personalization for peace: how algorithmic recommendations can impact conflict coverage.*

[17] WARREN, Samuel - BRANDEIS, Louis. The right to privacy. *Harvard Law Review*. 1890, Vol. 4, p. 193.

[18] HAAS, Claude. Privacy Protection through Publicity: Licensing Ones Likeness to Employers via Biometrics. *Albany Law Journal of Science & Technology*. 2025, Vol. 35.

[19] KOOPS, Bert-Jaap et al. A Typology of Privacy. *University of Pennsylvania Journal of International Law*. 2017, Vol. 38, p. 496.

long as the monitoring does not enable identification.[20] In such scenario, the individual anticipates the possibility of being seen but not recognized, and right to privacy remains largely relevant.

A further framework is provided by Daniel Solove, whose typology includes the concealment of certain matters from others, the ability to avoid unwanted interference, and the capacity to control the "life" of information about oneself. Solove also highlights intimacy and the protection of personality and dignity.[21] Beyond these conceptual dimensions, he provides a detailed categorization of privacy harms, encompassing physical, economic, and psychological harms, as well as relationship, discrimination, reputational, and autonomy-related harms,[22] which often rise from personal data processing. These categories serve as a useful lens for analysing the risks associated with the stages of personalization, from data collection through profiling, prediction, and content delivery.

Roger Clarke complements these perspectives by focusing on privacy in the context of technological development. He distinguishes privacy of personal behaviour, which concerns actions and activities that should remain within the individual's private sphere, and privacy of personal experience.[23] Everyday activities such as reading, purchasing books or media, engaging in conversations or attending small gatherings were invisible to others in the past. [24] In modern digital environments, however, these activities leave persistent records that may be accessed by others, thereby expanding the potential for privacy intrusion.[25]

In the context of personalisation, Solove's and Clarke's frameworks are particularly useful for identifying the multiple dimensions of privacy that may be affected. Solove's typology allows specific harms (informational, relational, autonomy-related, and reputational) to be mapped onto each stage of the personalization process. Clarke illustrates how the capture of personal behaviour and experience in digital environments extends the reach of privacy violations beyond traditional conceptions. Together, these perspectives emphasize that modern personalization technologies do not merely process data; they can affect autonomy, intimacy, and informational control, highlighting the need for careful legal and conceptual analysis.

III. PRIVATE LIFE IN THE DIGITAL AGE: THE ECHR'S EVOLVING APPROACH UNDER ARTICLE 8

The fundamental legal regulation concerning the right to privacy at the European level is the Convention for the Protection of Human Rights and Fundamental Freedoms (referred to as "Convention"). Article 8 contains a set of four closely related rights: the rights to respect for private life, family life, home, and correspondence.[26] In contrast, the

[20] Ibidem.
[21] SOLOVE, Daniel J. Conceptualizing Privacy. *California Law Review*. 2002, Vol. 90, p. 1092.
[22] SOLOVE, Daniel J. – CITRON, Danielle Keats. Privacy harms. *GW Law Faculty Publications & Other Works*. 2021.
[23] CLARKE, Roger. What's ‚Privacy'? In: *Xamax Consultancy Pty Ltd.* [online]. [2024-08-01]. Available at: http://www.rogerclarke.com/DV/Privacy.html.
[24] CLARKE, Roger. *Privacy.*
[25] Ibidem.
[26] The European Convention on Human Rights. In: *Council of Europe* [online]. [2024-08-08]. Available at: https://www.coe.int/en/web/human-rights-convention/private-life.

Charter of Fundamental Rights of the European Union (referred to as "Charter") protects the right to respect for private and family life, home, and communications in Article 7 but enshrines the right to the protection of personal data separately and explicitly in Article 8. Neither the Convention nor the Charter defines the concept of private life in greater detail; its meaning has therefore been developed through judicial interpretation.

The European Court of Human Rights (ECHR) adopts a broad interpretation of private life,[27] considering it a wider concept than privacy. It encompasses numerous spheres, ranging from an individual's health,[28] through interpersonal relationships that do not fall within family life,[29] to sexual life.[30] The open formulation allows the courts to adapt the interpretation of privacy to new circumstances requiring protection. At the same time, this broad protection is limited by the criteria of legality, proportionality, necessity, and legitimate interest, as conditions for permissible interference set out in the second paragraph of Article 8.[31] Because of the broad range of interests encompassed by private life, the ECHR has grouped relevant case law into three, possibly overlapping categories, including: the physical, psychological, or moral integrity of the person; privacy; and identity and autonomy.[32]

The ECHR consistently highlights that an exhaustive definition of private life is not possible.[33] Rather, private life encompasses the physical and psychological integrity of the person and includes many aspects of physical and social identity.[34] This open-ended approach ensures that the scope of Article 8 can flexibly adapt to social and technological developments.[35]

Technological developments have introduced new ways of processing personal data. The protection of personal data is closely linked to the protection of privacy and private life. For this reason, the ECHR stresses that the protection of personal data is essential for the effective protection of private life, including the processing of personal data within the scope of Article 8.[36] This protection may also extend to personal data already accessible in the public domain.[37] The ECHR further holds that users of telecommunications and

[27] KRATOCHVÍL, Jan. Kapitola XVIII [čl. 8 EÚLP]. In: Jiří Kmec et al. (eds.). *Evropská úmluva o lidských právech: komentář.* Praha: C. H. Beck, 2012, p. 867.

[28] Y. G. v. Russia, judgment of the European Court of Human Rights, 30. 11. 2022 No. 8647/12, 40-45.

[29] KILKELLY, Ursula. Handbook No. 1: The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights. Germany: Council of Europe, 2003, p. 11.

[30] Ibidem.

[31] PRUDENTOV, Roman V. Private Life and Surveillance in a Digital Era: Human Rights in European Perspective. *Digital Law Journal*. 2020, Vol. 1, No. 2.

[32] Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence. 2024, p. 31. In: *European Court of Human Rights* [online]. [2026-04-15]. Available at: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng.

[33] Niemietz v. Germany, judgment of the European Court of Human Rights, 16. 12. 1992 No. 13710/88, 29.

[34] Marper v. the United Kingdom, judgment of the European Court of Human Rights, 4. 12. 2008 No. 30562/04 a 30566/04, 66.

[35] *Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence,* p. 26.

[36] Rotaru v. Romania, judgment of the European Court of Human Rights, 4. 5. 2000 No. 28341/95.

[37] Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, judgment of the European Court of Human Rights, 17. 6. 2017 No. 931/13, 133-134.

internet services must have a guarantee that their privacy will be respected.[38] Although this guarantee is not absolute and must sometimes give way to other legitimate interests, such as crime prevention, online contexts require heightened sensitivity.[39] Information associated with dynamic IP addresses, for instance, typically enables the identification of a person and thus constitutes personal data not generally accessible to the public. The ECHR concluded that the use of such data falls within the scope of Article 8.[40] It also held that the applicant's expectation of privacy is not decisive in such circumstances, even if he did not conceal his dynamic IP address,[41] and in this regard highlighted the importance of user anonymity.[42] Ultimately, the ECHR's approach reflects the need to balance individual privacy with legitimate public interests, while adapting its interpretation to modern realities. By extending the scope of Article 8 to evolving contexts such as digital communications, the ECHR ensures that fundamental rights remain resilient and relevant in the face of technological change.

IV. PERSONALIZATION BEYOND CONVENIENCE: PRIVACY CONCERNS

Personalization relies on the acquisition and further processing of users' personal data, enabling profiling and the association of interests with an individual. The disclosure of personal information is, however, part of an individual's privacy, and each stage of the personalization therefore carries the potential to interfere with protected spheres of private life. The main activities involved in personalization can be grouped into four interconnected phases: the processing and collection of personal data (including the nature of data collected and the extent of monitoring), profiling, prediction, and the display of customized content. In this chapter, these steps will be analysed from privacy and data protection perspective.

Personal data processing constitutes the fundamental layer of personalization systems. The business strategies of contemporary digital markets are built upon the extraction and use of consumer data, which has become a major source of profit and market power. In the context of personalization, consent remains the only acceptable legal basis for processing personal data.[43] As the ECHR has long recognised personal data protection as falling within the scope of Article 8 of the Convention, the act of processing personal data itself – including simple data collection, constitutes an interference with an individual's private life.

A key aspect to consider in data collection is the principle of data minimization under GDPR, which requires companies to limit the scope, amount, and duration of personal data processing, especially in personalized advertising. This plays an important role in the context of personalization, as it limits the possibilities of tracking users and thus preventively reduces the interference with their privacy. The Schrems v. Meta decision

[38] Podchasov v. Russia, judgment of the European Court of Human Rights, 13. 5. 2024 No. 33696/19, 65.
[39] Ibidem.
[40] Benedik v. Slovenia, judgment of the European Court of Human Rights, 24. 4. 2018 No. 62357/14, 107-108.
[41] Ibidem, 116.
[42] Ibidem, 117.
[43] Judgment of the Court of Justice (Grand Chamber) of 4 July 2023, C-252/21.

reaffirmed that such processing must always be carried out carefully and must be justified on a case-by-case basis.[44] These requirements are especially strict for targeted advertising, where the use of sensitive data is rarely legitimate. As a result, companies are encouraged to rely on aggregated or non-identifiable data if possible. This approach not only reduces privacy risks but also aligns with GDPR's overarching goal of protecting individuals' rights.

In order to create a detailed profile that allows the display of the content which has the potential to attract consumers, it is beneficial for companies to collect as much personal data as possible. In addition to the amount of data collected, their type also plays a role. The collected personal data can, for example, indicate the health status of the consumer,[45] in the case where the data shows that the individual repeatedly purchases specific medicines or dietary supplements. Since health information falls within the privacy of a person according to the conclusions of the ECHR, the private life is being interfered with. Furthermore, health data constitutes sensitive personal data according to the GDPR, requiring heightened safeguards and justification. Personalization can also be based on GPS data and data about Wi-Fi connection. Users who have location tracking enabled reveal data about their location continuously.[46] This allows to track their movements and their daily routines and routes. In the case of tracking sports performance using smartwatches, information about regular movement routes can also be revealed.[47] Sports habits and leisure time activities are part of an individual's everyday life and reflect their private life, therefore their collection and use may constitute an interference with privacy and must be treated accordingly.

Monitoring represents a particularly intrusive dimension of personalization. Information about an individual is collected during every virtual interaction. Aware of such pervasive monitoring, individuals may begin avoiding certain actions or searches to prevent them from influencing future recommendations, a behavioural adaptation known as the "chilling effect".[48] This self-restriction undermines autonomy and hinders the free formation of identity. Continuous monitoring thus presents a more substantial interference with privacy than isolated instances of data collection, affecting core elements of private life and contradicting the possibility of being left alone or reaching the stage of Westin's solitude.

Profiling constitutes a distinct type of personal data processing. In personalization systems, profiling is an essential component which connects information to individuals, forming a basis for displaying a targeted content. The GDPR explicitly recognises profiling as a separate processing activity, particularly where it contributes to automated decision-making. Profiling also interferes with the individual's autonomy – since this is

[44] Judgment of the Court of Justice of 4 October 2024, C-446/21, 109 and 121.
[45] SAXENA, Ashish K. Balancing Privacy, Personalization, and Human Rights in the Digital Age. *Eigenpub Review of Science and Technology*. 2020, Vol. 4, No. 1, p. 28.
[46] TOCH, Eran et al. *Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems*, p. 209.
[47] BEN-SHAHAR, Omri. Data Pollution. *Coase-Sandor Working Paper Series in Law and Economics*. 2018, p. 113.
[48] HEMRSTRÜWER, Yoan - DICKERT, Stephan. Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten. *Social Science Research Network*. 2013, Vol. 15, p. 2.

the only content displayed to the user based on their profile,[49] their reactions serve as feedback to the algorithm, reinforcing patterns and distorting future behaviour.[50] In this way, personalization affects the privacy of personal behaviour in Clarke's sense.

All personalised content relies on predictions about what a user might want, need, or respond to in the future. These predictions are derived from behavioural profiling, from information on pages visited, products viewed or purchased, searches conducted, or even emails sent.[51] Predictions also incorporate socially derived data – information inferred from friends, relatives, roommates, or colleagues who share the same device, network, or account ("social-based personalization").[52] Private life includes individual's relationships beyond family relationships, as shown earlier with the ECHR decision. Prediction therefore also affects social relationships as part of private life. Moreover, it also affects right to informational self-determination, as the choices presented to users form their future behaviour. Inferred data go beyond explicit personal data or mere identifiers, as they do not rely solely on one's own data, but also on data relating to others, meaning that an individual's online experience can be shaped by information derived from the behaviour of those around them. This can interfere with an individual's privacy even where only a limited amount of their own personal data (possibly just an identifier) is directly processed.

The display of customised content represents the final stage of personalization, which I call personalization *stricto sensu*. The information presented through personalized content has substantial influence on the user's decision-making processes, behaviour, and attitudes. If predictions are inaccurate or if profiles are distorted, the personalized content shown may narrow user choice, reinforce biased assumptions, or reveal sensitive information to others, including friends, family, or colleagues,[53] thereby affecting the social sphere of privacy. More broadly, the cumulative effects of personalization raise concerns about autonomy, freedom of thought, and freedom of opinion, as individuals may encounter only a limited subset of available information.

These stages illustrate that personalization goes far beyond increased convenience. Each of its phase, from data collection and profiling to prediction and display, carries distinct privacy implications, and the interaction of all stages generates cumulative and often opaque forms of intrusion. Understanding these mechanisms is essential for assessing whether personalization practices remain compatible with the fundamental rights to privacy, autonomy, and informational self-determination.

[49] CAVENDER, B. The Personalization Puzzle. *Washington University Jurisprudence Review.* 2017, Vol. 10, p. 109.
[50] LEE, Jungkook - LEHTO, Xinran Y. E-personalization and online privacy features: the case with travel websites. *Journal of Management and Marketing Research.* 2010, p. 2.
[51] TOCH, Eran et al. *Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems*, p. 207.
[52] Ibidem, p. 204.
[53] Ibidem, p. 207.

V. PERSONALIZATION AS FORBIDDEN FORM OF AUTOMATED DECISION-MAKING UNDER GDPR

Article 22 of the GDPR presupposes presupposes processing of personal data relating to an identifiable data subject, creating a stronger tool for data protection involved in personalization. As such, it covers only such privacy concerns which arise from personal data protection. Indirectly, however, it protects other person's rights and interests by preventing decisions based solely on automated processing that could produce significant effects or otherwise adversely affect the individual's rights and freedoms, thereby limiting the risk of unjustified interference with broader fundamental rights beyond data protection itself.

A prerequisite for profiling is the monitoring of the characteristics of individuals. Due to the fact that the data create a profile of an identifiable person, these characteristics usually represent personal data. Their collection does not have to be automated. An example of non-automated profiling is the collection of CVs and conducting two rounds of interviews as part of the recruitment process. Profiling itself refers to the creation of profiles of individuals – a comprehensive overview of a person and their characteristics or interests. From the CV and from the information obtained during the interview, including applicant's behaviour, an HR professional creates a profile of the applicant, which is then compared with the profile of the ideal employee the company is looking for. From a CV, information disclosed during an interview, and observations of an applicant's conduct, an HR professional forms an evaluative profile and compares it with the profile of an ideal candidate. Profiles also occur in consumer contexts: they may reflect purchasing history, loyalty point usage, or the saving of favourite items in e-shops, where the profiling process is usually automated.

According to the GDPR, profiling constitutes a form of personal data processing which leads to the evaluation of certain criteria, enabling the controller to infer information such as economic status or personal preferences. Before the processing, the controller must comply with the transparency obligation regarding the nature of the processing when automated decision making (ADM) is involved. Profiling itself, however, does not trigger the additional duty to explain the logic and consequences of processing under Article 13(2)(f) GDPR, nor is profiling alone prohibited under Article 22 GDPR.

Unlike profiling, ADM is not explicitly defined in the GDPR. It can be understood as a decision carried out by technological means or algorithms.[54] "Decision" in this context does not refer exclusively to an individual legal act issued by a public authority. The guidelines of the former Working Party established under Article 29 (WP29; today's European Data Protection Board – EDPB) adopt a broader interpretation,[55] as well as the CJEU in its Schufa decision.[56] The term "individual" cannot be omitted. It suggests that some decisions will have collective or societal effects. The GDPR only applies to such decisions that will have an impact on specific data subject.

[54] European Data Protection Board. *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*. 2018, p. 8.
[55] Ibidem.
[56] Judgment of the Court of Justice of 7 December 2023, C-634/21.

Automated decision-making is not generally a priori prohibited by the GDPR. However, due to possible significant impact on the individual, it is regulated by Article 22. The first question related to Article 22 is the nature of the rule in question, as the article states that "the data subject shall have the right not to be subject to [automated individual decision-making] ...". This could therefore be either a right of the data subject as formulated in the article or a general prohibition of automated individual decision-making under the conditions further specified in Article 22. Although experts have addressed this issue,[57] the EDPB in its opinion clearly states that, despite the misleading formulation, the provision should be interpreted as a prohibition.

The wording of Article 22(1) suggests that the rule on automated individual decision-making applies only to significant situations. Although this may appear restrictive, many scenarios involve legal consequences. Legal effect, or legal consequence, is generally understood as an intervention in the rights and obligations of an individual, such as terminating a contract, granting or denying a social benefit, or refusing citizenship.[58] ADM performed by public authorities would typically have legal consequences, but legal effects also arise in private-sector contexts, for instance, in form of hiring decisions in private companies.

The concept of a "similarly significant effect" is deliberately broad and not defined by the GDPR. Recital 71 references examples such as automated rejection of loan applications or electronic recruitment processes without human involvement. These could lead to legal consequences (being granted a loan, becoming an employee). Given their negative outcome, the individual's initial situation does not change in essence, but has an indirect negative impact on him, such as the obligation to register with the employment office, failure to obtain certain benefits or payment of health insurance. As ECHR stated, a rejection of a profession has an effect of privacy, as profession is part of a human's private life.[59] A similarly significant effect therefore encompasses impacts that materially influence an individual's circumstances, behaviour, or opportunities, including potential psychological or economic harm. The criterion of "similarity" must be interpreted in relation to legal effects to maintain legal certainty and avoid subjective assessment based on individual perceptions of harm.

To facilitate interpretation, WP29 provides examples of decisions likely to be considered similarly significant, including those affecting financial status (e.g., credit eligibility), access to healthcare services, job opportunities, or admission to education.[60]

Although personalization is typically presented as a beneficial service to users, it simultaneously entails certain negative consequences. These harms share two characteristics.

---

[57] THOUVENIN, Florent et al. Article 22 GDPR on Automated Individual Decision-Making: Prohibition or Data Subject Right? *European Data Protection Law Review*. 2022, Vol. 8, No. 2, pp. 183–198.

[58] European Data Protection Board. *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, p. 8.

[59] Council of Europe. *Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Private and Family Life, Home and Correspondence*. 2024, p. 27.

[60] European Data Protection Board. *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, p. 8.

First, they are often difficult to detect, and second, their effects are challenging to prove, either because they are not easily quantifiable (e.g., addictive design mechanisms) or because, the harm is collective in nature.

Given that companies require a large amount of personal data for personalization, the first negative consequence can be seen as an intrusion into privacy. This intrusion is both extensive and intense. It is not only an intrusion into privacy by collecting personal data, nor merely a violation of informational self-determination. The first part of this article demonstrated the diverse ways in which personalization can invade privacy. As a component of privacy, autonomy of the data subject is limited by personalization.[61] Autonomy is a significant concept in private law, emphasizing individual freedom and choice. Personalization results in the shaping of the consumer's experience and choice options. Although it might seem that personalization now is ubiquitous and obvious to everyone, oftentimes users are not aware of this practice happening,[62] restricting control over their personal data and online experience.

Autonomy is closely related to biases enhanced in the personalization process.[63] Moreover, when a certain characteristic is detected and compared to other people's preferences, stereotypes are being strengthened within the algorithm and society. Consequently, the options which consumer is presented with can be distorted,[64] which leads to creation of echo chambers and rabbit holes, also known as filter bubbles.[65] Filter bubbles have a negative impact not only on the person's knowledge and access to information, but also on public discourse.[66] Filter bubbles and rabbit holes can lead to polarization, radicalization and fragmentation – these are especially possible if the personalized content involves topics such as politics or war.[67] However, maintaining balance is essential for cultivating an informed and engaged public, equipped with critical thinking skills and open to diverse perspectives.[68] These effects are not only sociological but also legally relevant. In particular, the restriction and shaping of user choice through personalization systems raises questions under Article 22 GDPR, which protects individuals from decisions based solely on automated processing that significantly affect them. If filter bubbles meaningfully influence users' access to information or decision-making capacity, they may contribute to such "significant effects," thereby triggering the need for safeguards under the GDPR.

[61] BASTIAN, Mariella. *News personalization for peace: how algorithmic recommendations can impact conflict coverage*, p. 316.
[62] Ibidem, p. 316.
[63] ALI, Muhhamad. Measuring and Mitigating Bias and Harm in Personalized Advertising. *Proceedings of the 15th ACM Conference on Recommender Systems*. 2021.
[64] Ibidem.
[65] BASTIAN, Mariella. *News personalization for peace: how algorithmic recommendations can impact conflict coverage*, p. 316.
[66] SAXENA, Ashish K. *Balancing Privacy, Personalization, and Human Rights in the Digital Age*, p. 55.
[67] BASTIAN, Mariella. *News personalization for peace: how algorithmic recommendations can impact conflict coverage*, p. 316.
[68] Ibidem.

CONCLUSION

Personalization is a sophisticated process that is based on the processing of excessive amount of personal data and interferes with various daily activities – writing emails, reading messages, using social networks, watching movies or videos. Although the ECHR has not yet directly addressed privacy concerns arising from personalization in its case law, its interpretations of the right to respect for private life provide a robust framework for examining privacy in the context of technological developments and the digital environment. Consequently, personalization can be meaningfully analysed through the lens of fundamental privacy rights.

This article has demonstrated that each stage of the personalization process interferes with the right to privacy. Importantly, it is not only the processing of personal data that constitutes an intrusion – personalization also affects broader dimensions of privacy, including aspects beyond informational self-determination. These dimensions encompass Westin's concepts of anonymity and solitude as well as Clarke's notions of the privacy of personal experience and privacy of personal behaviour.

Among existing privacy frameworks, Clarke's privacy of personal experience is particularly relevant to understanding the challenges faced by users consuming personalized content. Moreover, Solove's taxonomy of privacy harms effectively categorizes the ways in which personalization can generate harm. However, it is crucial to acknowledge that not every interference with private life constitutes a violation of the right to respect for private life, and conversely, not every GDPR violation equates to a privacy violation. Such legal assessments need to undergo case-by-case analysis. Personalization, in all its forms and stages, represents an interference with individuals' private life. These processes particularly affect autonomy, informational self-determination, interpersonal relationships, and anonymity, which are core components of the broader concept of privacy. Addressing this interference requires careful consideration of data collection practices, including inferred data, and transparency in profiling mechanisms.

While the GDPR provides a framework for the protection of personal data, it cannot exhaustively address all issues arising from personalization practices. Especially it does not, and it was not inteded to, encompass all dimensions of privacy. In particular, situations in which an individual's privacy interests are intertwined with or dependent upon the personal data of others show structural limits within a purely data-protection-based approach. Although Article 22 protects a person from significant impacts on his rights, including privacy, its aplicability is limited and based on strict personal data processing. These limitations suggest that a broader interpretation of Article 22 alone is insufficient to safeguard the full spectrum of privacy. However, judicial developments offer a compelling base for acknowledgement of the wide range of dimensions of privacy. By drawing on broader human rights principles, courts have begun to articulate a more holistic understanding of privacy that justifies and supports a wider, more protective interpretative approach.