UDK 342.721:004.738.5]:340.131
316.47:004.738.5]:342.721
Review article

CHALLENGES OF PERSONAL DATA PROTECTION ON THE INTERNET -IMPACT ON DEMOCRACY, PUBLIC ADMINISTRATION AND THE RULE OF LAW IN THE EU

Mirko Klarić, PhD, Full Professor
University of Split, Faculty of Law
Domovinskog rata 8, 21 000 Split, Croatia
mirko.klaric@pravst.hr

Maja Proso, PhD, Associate Professor
University of Split, Faculty of Law
Domovinskog rata 8, 21 000 Split, Croatia
maja.proso@gmail.com

ABSTRACT

Rapid development of information and communication technologies brings many challenges and risks for the protection of personal data since the internet has become enormously influential in virtually every aspect of daily life. Privacy and data protection are interrelated since data protection is a legal mechanism that ensures privacy of the subject on the Internet. Privacy is a fundamental human right, recognized in many international and regional human rights documents. The misuse of technologies has just recently shed some light on the meaning and importance of this subjective right in contemporary societies, and has also pointed to the problem of defining its content in context of informational and technological development. Digital transformation also affects the way how companies analyse consumer preferences in order to create personalized ads. The paper examines the right to privacy of personal data, existing legal framework for the protection of privacy and personal data and its impact on the rule of law in the EU, focusing on the examining of existing rules on processing personal data on the Internet, particularly legal regulation and challenges of processing personal data for the purpose of profiling and behavioral advertising on the Internet, using cookies. By processing data, companies on the Internet aim to develop new advertisements, products, and services specified to the particular consumer needs. Recent landmark decision of the Court of Justice of the European Union C – 252/21, (Meta Platforms and Others v. Bundeskartellamt) is analyzed as well, because it clarifies several points of data protection law, namely GDPR, regarding personalized use of

consumers' personal data for behavioral advertising on social network platforms. The Court of Justice of the European Union made it clear that the personalization of advertising financed by the Internet social network Facebook cannot justify the processing of (sensitive) data if there is no consent given by the data subject. According to development of legislation of the European Council and the European Parliament and legal practice of the Court of Justice in digital transformation development, personal data protection became more significant and important part of regulatory framework the European Single Market. This regulation specific influences on approach and acting of public institutions, governmental bodies and private entities in personal data protection. This paper will analyze how challenges of personal data protection can influence on public institutions activity and citizens' rights in two fields of regulation: access to personal data and possibility of collecting, using and manipulation of personal data with role of public institutions in personal data protection.

***Keywords**: Court of Justice of the European Union, personal data protection, Internet, the rule of law, public institutions*

1. INTRODUCTION

The age in which we live is predominantly digital, informational and communicative in nature. The Internet transmits information on a global scale, therefore information security plays an important role. Technological devices used for communication and Internet access leave virtual traces through which the user can be identified and his/her personal data can be used illegally. Today, social networks are possibly the biggest transmitters of information (therefore personal data) today. By collecting users' personal data and monitoring their activities, the owners of social networks profile use them for the purpose of targeted advertising or, alternatively, forward their personal data to third parties, without permission. The increasing availability of personal data and the possibility that, due to technological development, data is exchanged and used globally carries with it the risk of its unauthorized collection, processing and transfer. This seriously jeopardizes the individual's informational personality.[1] It implies that the individual decides whether, when, to whom, how much and how to communicate his/her personal data. Thus, the German Constitutional Court in 1983 accepted the concept of information personality as an individual's right to independently decide when and to what extent information about his/her private life can be disclosed to others. Of course, such authorization is not unlimited, given that the right to protect personal data is subject to limitations in cases of public interest and (cumulatively) when

[1] The concept of information personality was defined by Alan Westin in 1970. as "the requirement of individuals, groups or institutions to independently decide when, how and what information about themselves will be given to others „, Westin, A., *Privacy and Freedom*, New York, Atheneum, 1970., p. 7 in: Brezak, M., Pravo na osobnost, Pravna zaštita osobnih podataka od zlouporabe, Zagreb, Nakladni zavod Matice Hrvatske, 1998, p. 22.

the stated limitations are prescribed by law, clear and proportionate.[2] The right to protection of personal data is recognized as a fundamental right in Article 8 of the Charter of Fundamental Rights of the European Union (further: Charter).[3] The Charter confirms the right to the protection of personal data and the fundamental values associated with this right are presented. It establishes that the processing of personal data must be fair, that it must be carried out for established purposes and be based on the consent of the person in question or on a legitimate basis established by law. Individuals must have the right to access their personal data and the right to correct it, and the observance of this right must be subject to the supervision of an independent body. The right to protect personal data exists precisely with the aim of enabling an easier flow of information, while protecting the personal data of individuals.

The protection of personal data aims to achieve the transparency of all other non-private data.[4] The protection of personal data is considered a modern and active right[5] which establishes a system of checks and controls in order to protect individuals during each processing of their data.

2. INSTITUTIONAL FRAMEWORK OF PERSONAL DATA PROTECTION WITH MAIN PRINCIPLES

Democratic advantages of personal data protection are an important part in the development of information security for citizens not only on the Internet, but also in other aspects of daily life.[6] A significant number of citizens are concerned about their privacy and protection of their private life. This trend depends on development in various aspects of information technologies, where the possibilities of interactive communications are growing, according to technological solutions.[7] The

---

2 Kiss, A.; Szoke, G. L., *Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation*, in: Gutwirth, S.; Leenes, R.; de Hert, P., (eds.), Reforming European Data Protection Law, Springer International Publishing AG, 2015, pp. 314-315.

3 European Union Charter of Fundamental Rights, Official Journal of the European Union, C 326.

4 Bosco, F., *et al., Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and perspectives from European Data Protection Authorities*, in: Gutwirth, S.; Leenes, R.; de Hert, P., (eds.), Reforming European Data Protection Law, Springer International Publishing AG, 2015, p. 17.

5 Independent lawyer Sharpston stated that the case involves two separate rights: the "classic" right to privacy protection and the "more modern" right to data protection. Joined Cases C-92/09 and C-93/02, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, Opinion of Independent Counsel Sharpston, 17 June 2010, p. 71.

6 Fuster, G. G., *The emergence of personal data protection as a fundamental right of the EU*, Springer International Publishing Switzerland, 2014, pp. 185 – 204.

7 Kulhari, S., *Builduing-Blocks of a Dana Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity*, Nomos Verlagsgesellschaft mbH, Baden-Baden, 2018, pp. 23–37.

development of social media and social networks with the creation of interactive connections between various data basis and relatively simple publication of data makes users vulnerable from possible abuse of information technologies.[8] Personal data are more accessible and available according to modern technological tools which enable immediate publication and dissemination in the public space. The development of AI technology solutions brings new possibilities in accessibility, processing, storage and manipulation of personal data. Relatively simple AI technological tools available on the Internet enable the processing and analysis of data available through social networks, which can potentially threaten the privacy of the citizens as one of the fundamental human rights. The principles for the control of personal data sharing and dissemination have been developed to protect people from the consequences of uncontrolled data publishing with personal elements.[9] Those principles have universal characteristics focused on various aspects of personal data protection: potential availability, possibility of access, processing and manipulation of personal data, dissemination and protection of special, vulnerable categories of personal data. Every aspect of personal data use is important in developing the main principles of data protection and their division from other types of data, which are not of a personal character.

There are several principles created from the public policy approach, according to the restrictions of personal data access: the principle of data personalization, the principle of protection of personal data dissemination, the principle of diversification of personal data protection, the principle of limited access to personalized data and the principle of special protection of vulnerable categories of personalized data.[10]

The principle of data personalization includes the approach to specific and certain information which identifies or can identify some person. This principle tries to harmonize two main requests: firstly, the right of the public to have access to all information connected with activities with public dimension, and secondly, a

---

8 Custers, B., *et al., Introduction*, in Custers, B., *et.al.*, *EU Personal Data Protection in Policy and Practice. Information Technology and Law Series*, vol 29. T.M.C. Asser Press, The Hague. 2019, Springer, pp. 1–16.

9 Roos, A., *5 Core Principles of Data Protection Law*, The Comparative and International Law Journal of Southern Africa, Vol. 30, No 1., 2006, pp. 102–130.

10 There are also division principles of personal data protection, according to the Article 5 of GDPR: principle of transparency and lawfulness, principle of accountability, principle of confidentiality, principle of data minimization, principle of accuracy, principle of storage limitation and principle of purpose limitation. These principles concretize main start points for shaping the EU regulatory framework for the protection of personal data. Another division of personal data protection principles are developed according to the main elements of the personal data protection, which are common to all legal systems, and depend on specific characteristics of personal data itself and their sensitivity.

special approach to data connected to a specific person. The first request is connected with the activity and functioning of public authorities, central and local government administration and public institutions. The second request is focused on privacy protection of the persons included in public activities in the part which does not include their public engagement. Those data, with specific informational elements which can identify certain specific personal characteristics of a concrete person, represent personal data and they are subject to special restrictions in legal transactions and their availability to the public. The importance of this principle has been growing lately, according to development of new information technologies, including artificial intelligence.[11] By implementation of the new information technologies, it is relatively simple to manipulate personal data, or abuse them, including the possibilities such as face and voice recognition and identification.[12] The development of new artificial intelligence technology solutions opens many various manipulation possibilities with personal data modification.[13] That induces development of various regulatory tools to protect citizens from possible manipulations of their personal data and intrusion into their privacy.[14] Implementation of this principle is focused on developing criteria for demarcation between data that fall into the public sphere and are subject to public criticism, from information which is, in principle, in the private sphere of individuals involved in public affairs.[15]

The principle of protection of personal data dissemination describes limits which can be set in data protection policy in order to limit access to vulnerable data which identify or can identify individual persons.[16] Personal data dissemination is the second challenge in regulation, mostly because clear differentiation between public data and personal data does not exist. It is obvious that at the same time in public data exist which can be, according to their characteristics, described as public data, and at the same time, data which can be described as personal data.

---

11 Aliyev, I. A.; Rzayev, G. A.; Ibrahimova, A. N., *Artificial Intelligence and Personal Data: International and National Framework*, Peace Human Rights Governance, Vol. 5., No. 1., 2021, pp. 97–123.

12 Czerniawski, M., de Hert, P., *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*, International Dana Privacy Law, Vol. 6., No. 3., 2016, pp. 230 –243.

13 Humerick, M., *Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence Comments*, Santa Clara High Technology Law Journal, Vol. 34, No. 1., 2018, pp. 393–418.

14 Elvy, S. A., *Paying for Privacy and Personal Dana Economy*, Columbia Law Review, Vol. 117, No. 6., 2017, pp. 1369–1459.

15 Žliobaitė, I.; Custers, B., *Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models*, Artificial Intelligence and Law, Vol. 24, No. 2, 2016, pp. 183–201.

16 Belanger, F., Crossler, R. E., Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems, MIS Quarterly, Vol. 35., No. 4., 2011, pp. 1017. – 1041.

By implementation of modern information technologies, possibilities of data dissemination are huge and difficult to control, and after dissemination it is impossible to stop using that information. To implement the principle of personal data dissemination one needs to prepare and develop criteria for differentiation between public and personal data, for the protection of spreading personal data in the public space.[17] Implementation of criteria for the protection of personal data dissemination is an important previous step that ensures the full application of the principle of publicity and control of the public, while simultaneously protecting the right to privacy of citizens as one of the fundamental human rights. The only way for efficient limitation of dissemination of personal data is a regulative framework with incorporated consistent and implementable criteria for division between public and personal data. It is especially important in situations where personal data has public influence and affects social and political relations in the community. In that case, it is important to evaluate in which occasions it is necessary to limit access to data which include personal and public elements and how to divide public from personal in daily data politics. The principle of diversification of personal data protection includes development of various regulatory tools to increase personal data protection. The tools important for personal data protection include three types of potential measures: penal, misdemeanor and material. Penal measures include the possibility of criminal prosecution, misdemeanor includes a milder form of responsibility than criminal liability, but sanctions which are mostly financial penalties, and the third type of measures is focused on liability for damage caused by potential abuse of personal data protection.

The principle of limited access to personalized data is focused on developing criteria for access to personal data. Some of the personal data are mostly connected with the private life of the identifying person, and they are separated from the public, social, economic or political position of the person in society.[18] Other types of personalized data, which are accessible in the public sector can identify a certain person in a specific social role, such as economic or political status, public position and influence social relations and community movements, etc. Those data are mostly related to the public sphere and can be important because of the principles of openness and transparency in the activity of public bodies and institutions. It is necessary to describe procedure mechanisms to divide public elements from private elements in personalized data according to the principles which guarantee

---

17 Custers, B., *et al., A comparison of data protection legislation and policies across the EU*, Computer Law & Security Review, Vol. 34., No. 2., 2018, pp. 234 –243.

18 Hallinan, D.; Friedewald, M.; McCarthy, P., *Citizens' perceptions of data protection and privacy in Europe*, Computer Law & Security Review, Vol. 28., No. 3., 2012, pp. 263–272.

the open and transparent work of public authorities. Those procedures assure the implementation of the right to access information held by public authorities.

The principle of special protection of vulnerable categories of personalized data is focused on personal data types with specific characteristics such as gender, race, ethnic origin, religious affiliation, ideological or political orientation and health conditions, etc. According to the specific characteristics of data, limitation of data access and specific conditions in data collecting and processing is provided.[19] These conditions are important to especially protect vulnerable categories of personal data of abuse or malicious use, which is important in order to protect the dignity and self-respect of addressed people. The principle of special protection of vulnerable categories besides its interest dimension has also the technical dimension, which describes procedures important for special protection of data. The interest dimension of protection defines which type of personalized data can be identified as vulnerable, with a specific approach to their protection. The technical dimension of vulnerable categories personalized data protection includes specific legal measures, which are needed to protect access, manipulation and dissemination in their daily manipulation. This protection is at the focus of special interest, in order to promote and improve human rights in contemporary society.[20]

3. LEGAL FRAMEWORK OF PERSONAL DATA PROTECTION

With the development of information technology, the need for legal protection by regulations to protect the personal data of individuals grew as well.[21] Article 12 of the General Declaration on Human Rights[22] on respect for private and family life meant that for the first time an international legal instrument established the right of an individual to protect his/her private sphere from the interference of others, especially the state. Although by its nature it is a non-binding legal act, the Declaration influenced the further development of legal protection of human rights in Europe. The right to protection of personal data is part of the rights protected by Article 8 of the European Convention on Human Rights (further: the Conven-

---

19 Hall, L. B.; Clapton, W., *Programming the machine: Gender, race, sexuality, AI, and the construction of credibility and deceit at the border*, Internet Policy Review, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 10, No. 4, 2021, pp. 1–23.

20 Van Dijk, N., *et al., Right engineering? The redesign of privacy and personal data protection, International Review of Law*, Computers & Technology, Vol. 32, No. 2 – 3., 2018, pp. 230–256.

21 The European Court of Justice has expanded the definition of personal data to include dynamic IP addresses. See: Case C-582/14 *Breyer v Bundesrepublik Deutschland* ECLI:EU:C:2016:779., [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582], Accessed 24 May 2024.

22 United Nations (UN), Universal Declaration of Human Rights, December 10, 1948.

tion[23]) which guarantees the right to respect private and family life, home and correspondence, and prescribes the conditions under which limitations of this right are allowed. In the mid-70s, the Committee of Ministers of the Council of Europe passed several resolutions on the protection of personal data, referring to Article 8 of the Convention.[24] Convention on the Protection of Individuals in the Automatic Processing of Personal Data (further: Convention No. 108)[25] up to this day remains the only legally binding international instrument in the field of data protection[26]. Convention no. 108 applies to all data processing in the private and public sector, including processing in the judiciary and processing performed by bodies responsible for the execution of legislation. The convention protects individuals from misuse when processing personal data and at the same time seeks to regulate cross-border transfers of personal data. With regard to the processing of personal data, the principles from the Convention particularly concern the fair and lawful collection and automatic processing of data for certain legitimate purposes.[27] The Charter of the European Union on Fundamental Rights of 2000 with the enforcement of the Treaty of Lisbon in 2009 became legally binding as primary EU law. Adoption of the Treaty of Lisbon is a turning point in the development of legislation on data protection, not only because of the elevation of the Charter to the level of a legally binding document of primary law, but also because of ensuring the right to the protection of personal data. This right is expressly established in Article 16 of the TFEU, in the part of the Treaty dedicated to the general principles of the EU. Article 16 also creates a new legal basis that gives the EU the competence to pass laws on data protection issues. This is important because EU data protection regulations, especially the Data Protection Directive, were originally based on the legal basis of the internal market and the need to harmonize national laws so that the free movement of data in the EU would not be restricted.[28] >From 1995 to 2018, the legal instrument of the EU in relation to data protection was Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free flow of such data (further: Data Protec-

---

23 The European Council, European Convention on Human Rights, CETS br. 005, 1950.

24 Council of Europe, Committee of Ministers (1973), Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector, 26 September 1973; Council of Europe, Committee of Ministers (1974), Resolution (74) 29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector, 20 September 1974.

25 Council of Europe, Convention on the Protection of Individuals with Automatic Processing of Personal Data, CETS br. 108, 1981.

26 *Handbook on European Data Protection Legislation*, Luxembourg: Publications Office of the European Union, 2020, p. 26.

27 *Ibid.*

28 *Handbook on European Data Protection Legislation*, *op.cit.*, note 10, p. 30.

tion Directive).[29] The data protection directive established a detailed and comprehensive data protection system in the EU. The directives are transposed into national legislation, which in practice has resulted in a mismatch of legal rules for the protection of personal data at the EU level. This fact, along with the constant and rapid development of information technologies, led to the need to reform legislation on data protection in the EU. The reform resulted in the adoption of Regulation (EU) 2016/679 on the protection of individuals in relation to the processing of personal data and on the free movement of such data and on the repeal of Directive 95/46/EC.[30] Unlike the Directive, the Regulation is a horizontal source of personal data protection rights, which means that it is fully binding and directly applicable in all member states. The way in which the territorial scope of application of the Regulation is arranged results in the potential global effect of its provisions, especially for issues of online business where the subject of processing is the personal data of EU citizens.[31] The material area of application of the General Regulation includes processing of personal data that is fully automated and non-automated processing of personal data that are part of the storage system or are intended to be part of the storage system.[32] The GDPR Regulation contains definitions of terms important for the interpretation of its field of application. It thus defines personal data as all data relating to an individual whose identity has been determined or can be determined, i.e. a person who can be identified directly or indirectly, especially with the help of identifiers such as name, identification number, location data, network identifier or with the help of one or more factors inherent in the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.[33] Some of the novelties brought by the GDPR Regulation are the introduction of the term network identifier into the definition of personal data and, for the first time, in the following text, the legal definition and regulation of genetic and biometric data as personal data.[34] In the field of electronic communication, the possibility of unjustified interference in the user's personal sphere has increased due to the advanced possibilities of eavesdropping and

---

29 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free flow of such data, OJ 1995 L 281.

30 Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals in connection with the processing of personal data and on the free movement of such data and on the repeal of Directive 95/46/EC (further: Regulation GDPR), OJ L 119/1.

31 Gumzej, N., *Uredba o zaštiti osobnih podataka*, 2017, Projekt "Novi hrvatski pravni sustav" Pravnog fakulteta Sveučilišta u Zagrebu, p. 2.

32 Art. 2. par. 1. GDPR.

33 Art. 2. par. 1. GDPR .

34 Čizmić, J.; Boban, M., *Učinak nove EU Uredbe 2016/679 (GDPR) na zaštitu osobnih podataka u Republici Hrvatskoj*, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 39, br. 1, 377-410, 2018, p. 382.

monitoring of communication. For this reason, it was considered that special regulations on data protection are necessary in order to eliminate certain risks to which users of communication services are exposed.[35] As part of the EU legal framework, in order to complement and adapt the provisions of the former Directive on data protection in the telecommunications sector, the Privacy and Electronic Communications Directive (hereinafter: the e-Privacy Directive) was adopted in 2002 and amended in 2009.[36] The e-Privacy Directive applies to communication services in public electronic networks. In the e-Privacy Directive, three main categories of data generated during communication are distinguished. These are: data that make up the content of messages sent during communication, data necessary for the establishment and maintenance of communication, so-called metadata, which in the Directive is called "traffic data", such as information about the people who communicate, the time and duration of communication, and metadata includes data specifically related to the location of the communication device, so-called location data - this data is also data on the location of the user of the communication device, especially when it comes to users of mobile communication devices.[37] In January 2017, the European Commission adopted a new Proposal for a regulation on e-privacy[38] which replaced the e-Privacy Directive. The main goal of the proposed regulation is the protection of the fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communication services, especially the right to respect private life and communication and the protection of natural persons in regard to the processing of personal data. The proposed regulation simultaneously ensured the free movement of electronic communication data and electronic communication services within the Union. While the GDPR regulation primarily refers to Article 8 of the EU Charter of Fundamental Rights, the proposed regulation seeks to incorporate Article 7 of the Charter into the secondary law of the Union. The proposed regulation also adapts to new technologies and the market with the aim of building a

---

35 *Handbook on European Data Protection Legislation*, *op.cit.*, note 10, p. 332.

36 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of privacy in the field of electronic communications, SL 2002 L 201 (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and the Council of November 25, 2009 amending Directive 2002/22/EC on universal services and user rights with regard to electronic communications networks and services, Directive 2002/58/EC on the processing of personal data and protection of privacy in the electronic communications sector (further: Universal Services Directive) and Regulation (EC) no. 2006/2004 on cooperation between national authorities responsible for the implementation of laws on consumer protection, OJ 2009 L 337.

37 *Handbook on European Data Protection*, *op.cit.*, note 10, p. 334.

38 Proposal for a regulation of the European Parliament and the Council on respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on privacy and electronic communications) (COM(2017) 10 final), Art. 1.

comprehensive and consistent legal framework. The e-Privacy Regulation would therefore be the *lex specialis* in relation to the GDPR Regulation. The e-Privacy Regulation covers the processing of "electronic communications data", including the content of electronic communications and metadata that are not of a personal nature. The scope is limited to the EU, including cases where data collected in the EU is processed outside the EU and extends to the so-called OTT communication providers (over the top). These are service providers that deliver content, services or applications over the Internet without the direct involvement of a network operator or internet service provider. Examples of such service providers are globally known Skype, WhatsApp, Google, Spotify and Netflix. The implementation mechanisms of the GDPR Regulation would also apply to the new Regulation.[39]

4. CHALLENGES OF PROCESSING PERSONAL DATA FOR THE PURPOSE OF PROFILING AND PERSONALIZED ADVERTISING ON THE INTERNET

Along with the development of digital marketing and personalized advertising, the concern of users about their privacy on the Internet also grew. The collection of data on the Internet had to be legally regulated so that users would have additional security.

4.1. Processing of personal data through cookies

The term "cookies" refers to a text file that certain internet servers save on a computer or mobile phone when visiting web pages. "Cookies" are managed by the Internet browser. Cookies are small text files that websites place on your device while you are browsing. They are processed and stored by your web browser. In and of themselves, cookies are harmless and serve crucial functions for websites. Cookies can also generally be easily viewed and deleted. However, cookies can store a wealth of data, enough to potentially identify you without your consent. Cookies are the primary tool that advertisers use to track your online activity so that they can target you with highly specific ads. Given the amount of data that cookies can contain, they can be considered personal data in certain circumstances. When people complain about the privacy risks presented by cookies, they are generally speaking about third-party, persistent, marketing cookies. These cookies can contain significant amounts of information about your online activity, preferences, and location. The chain of responsibility (who can access cookies' data) for a third-party cookie can get complicated as well, only heightening their potential

[39] *Handbook on European Data Protection*, *op.cit.,* note 10, p. 336.

for abuse. GDPR is the most comprehensive data protection legislation that has been passed by any governing body to this point. However, it only mentions cookies directly once, in Recital 30.[40] The processing of personal data through cookies in the legislative framework of the European Union is prescribed by the Directive on e-Privacy and the Directive on Universal Services. In the Republic of Croatia, the directives were implemented in the Electronic Communications Act (further: ZEK).[41]. By provision of Article Art. 43, paragraph 4 of the ZEK it is stipulated that the use of electronic communication networks for data storage or for access to already stored data in the terminal equipment of subscribers or service users is allowed only in the event that the subscriber or service user has given his/her consent, after receiving clear and complete notification in accordance with special regulations on the protection of personal data, particularly on the purposes of data processing. This cannot prevent the technical storage of data or access to data solely for the purpose of transmitting communications via an electronic communications network, or, if necessary, for the purpose of providing information society services at the express request of subscribers or service users. The legal basis for the collection of personal data using cookies, which are stored on the user's computer/terminal equipment, is the user's consent, which should be in compliance with the provisions of the GDPR, Article 4, Paragraph 1, Point 11, which defines consent as any voluntary, in particular, informed and unequivocal expression of the wishes of the subject by which s/he consents to the processing of personal data relating to him/her by a statement or a clear affirmative action. In the judgment of the Court of the European Union in case C-637/17[42] the court established guidelines for consent that are considered valid and a pre-selected checkbox on a website does not constitute valid consent. Thus, the consent must be active and explicit, given for each of the separate purposes, so that it should not be interpreted differently depending on whether it is personal or non-personal data and it cannot be implied that the consent was given by undertaking some other activities. Direct marketing and tracking consumer behavior (profiling) are key tools that a company can use to sell its product or service.

---

40 „Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."

41 Official Gazette no. 76/22.

42 Court of Justice of the European Union, Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v. Planet49 GmbH, Case C-673/17, para. 66-71. [https://eur-lex.europa.eu/legal-content/hr/TXT/?uri=CELEX:62017CC0673] Accessed 2 February 2024.

4.2. Profiling

Technological development in the field of electronic communications and information and communication technologies has made it possible to identify, monitor and analyze user behavior by storing data generated by the use of electronic communications and communication services.[43] The GDPR defines profiling as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects related to an individual, in particular to analyze or predict aspects related to work performance, economic condition, health, personal preferences, interests, reliability, behavior, location or movement of that individual.[44] Network identifiers on user devices leave traces of user activity on the Internet which, especially in combination with unique identifiers and other information received by servers, can be used to create profiles of individuals and identify them. The most common form of profiling is based on the so-called "tracking cookie" technology, where the cookie is stored on the user's terminal equipment. The first step in profiling is data collection using tracking technologies.[45] The second step of profiling is creating a user profile. Collected data is analyzed using statistical correlation software that creates profiles by combining these data through the analysis of specific patterns of behavior.[46] Using cookies, user behavior is monitored (for example, which internet content the user prefers), with the aim of creating marketing ads that would be interesting and attractive to a certain user.

4.3. Personalized (targeted) advertising

The emergence of the Internet enabled more efficient and cheaper advertising to a wide range of users. Marketing, as a process of continuous activity that constantly adapts to economic, socio-economic, ecological, political and other trends, takes on new forms in its development, one of which is direct marketing, which was created as a result of a new approach to market business focused on the individual who wants his/her personality to be respected.[47] For successful targeted advertising, it is important to collect data about potential and current consumers in order to create a quality database and use it for a successful targeted advertising

---

43 Gumzej, N., *Challenges of the digital environment for personal data privacy and security*, Društvo i tehnologija 2014., p. 707.

44 Article 4., par. 4. GDPR.

45 Kamara, I.; Kosta, E., *Do Not Track initiatives: regaining the lost user control*, International Data Privacy Law, vol. 6., Issue 4, 2016, p. 6.

46 Kamara,; Kosta, *op.cit.*, note 29, p. 7.

47 Sudar, Kulčar, M., *Zaštita privatnosti i sigurnosti pohranjenih podataka s osvrtom na izravni (direktni) marketing,* Politička misao, vol. XLII, 2005., no. 4, p.105.

campaign.[48] Their behavior whether captured during a sales call , or measured at-scale by an activity like a web site visit, represents an incredible moment of insight for the marketer savy enough to listen closely and act on that information.[49] An example of targeted advertising is a situation when an advertiser requests from a social network to display an ad to respondents who meet certain criteria (age, gender, place of residence) at a specific time of day. The social network uses the personal data of its users to develop criteria that allow the advertiser to direct the ad to potential users.

4.4. Legal regulation of cookies for processing personal data for the purpose of profiling and behavioral advertising

The use of cookies is regulated in the EU by the provisions of The e-Privacy Directive from 2002, which, as mentioned earlier, was significantly amended in 2009. The provisions of both Directives were transposed into the national legislation of the Republic of Croatia via ZEK. That's how the so-called cookie rule contained in the provision of the article. 43, paragraph 4 of the ZEK.[50] Installing cookies and reading already stored information about an individual on the terminal equipment may only be done with consent and prior clear information that the data will be collected and for what purpose, and in accordance with regulations on personal data protection. Only cookies that are technically necessary for the development of communication between the user's terminal equipment and the Internet site he visits or for the provision of a service at the user's request are exempt from consent.[51] Cookies exempt from consent are mainly "user input" cookies, authentication cookies, security cookies, media player session cookies, load balancing session cookies, and cookies for sharing user content on social networks via social network plugins[52]. Installing cookies and reading already stored information about an individual on the terminal equipment may only be done with his/her consent and

---

48 *Ibid.*

49 Walters, D., *Behavioral Marketing: Delivering Personalized Experiences at Scale*, New Jersey, 2015, p. 3.

50 "The use of electronic communication networks to store data or to access data already stored in the terminal equipment of the end user or users is permitted only in the case when that end user or user has given his consent, after receiving clear and complete notification in accordance with the regulations on protection of personal data, especially on the purposes of data processing. This cannot prevent the technical storage of data or access to data solely for the purpose of carrying out the transmission of communications via an electronic communication network, or, if necessary, for the purpose of providing information society services at the express request of the end user or users."

51 *A cookie guide for micro, small and medium-sized businesses*, Agency for the Protection of Personal Data (AZOP), 2022, p. 4. [https://azop.hr/wp-content/uploads/2022/01/Vodic-za-kolacice.pdf], Accessed 3 February 2024.

52 *Ibid.*

prior clear information that the data will be collected and for what purpose, and in accordance with the regulations on personal data protection. Only cookies that are technically necessary for the development of communication between the user's terminal equipment and the Internet site they visit or the provision of services on the Internet site at the user's request are exempt from consent.[53] Pursuant to the provisions of The e-Privacy Directive and ZEK, if a cookie from a group of cookies for which consent is not requested [54] processes personal data, it is necessary to provide the user/respondent with information about the processing of personal data in accordance with the principle of "legality, fairness and transparency" of the GDPR.[55] According to Recital 47 of the GDPR, the processing of personal data for direct marketing purposes may fall under clause of legitimate interest.[56] Likewise, in Case C-131/12[57], the European Court of Justice took for granted that economic interests are legitimate interests[58]. GDPR stipulates that consent must meet all the conditions stipulated in Article 7 of the GDPR and, among other things, it must not be conditional. It must be explained to the user in clear and simple language what scope of personal data will be collected and for what purpose, and enable him/her to decide for him/herself whether s/he consents to the processing of that scope of data or not. According to the GDPR, consent should be given for each type of cookie according to their functionality separately, i.e. consent cannot be unified for all types of cookies.[59] The user has the right to withdraw the given consent in the same (simple) way.[60] The user also has the right to object to the processing of personal data by submitting an objection,[61] especially if the profiling is done for the purpose of direct marketing.[62] The user, therefore, cannot object to profiling when the legal basis for the processing of consent is the

---

53 *Ibid.*

54 Cookies that are technically necessary for the communication between the user's terminal equipment and the Internet site he visits or the provision of a service on the Internet site at the user's request do not require consent, such as "User input" cookies, authentication cookies, user-oriented security cookies, multimedia player session cookies, load balancing session cookies, cookies for sharing user content on social networks via social network plugins.

55 A cookie guide for micro, small and medium-sized businesses, *op.cit.*, note 35, p.7.

56 Recital 47. GDPR: „The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. "

57 Case C-131/12, Google Spain,13 May 2014, ECLI:EU:C:2014:317, [https://curia.europa.eu/juris/document/document.jsf;jsessionid=70B5FAE5A59EBF9E4D3284E3D55099C9?text=&docid=138782&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=543544]3,Accessed 25 May 2024.

58 Case C-131/12, para. 81.

59 A cookie guide for micro, small and medium-sized businesses, *op.cit.,* note 35, p.8.

60 Art. 7. par 3. GDPR.

61 Art. 21. GDPR.

62 Art. 21., par 2. GDPR.

execution of a contract or another basis, which excludes a significant number of cases of profiling.[63] Unlike profiling, it is possible to object to data processing for the purpose of direct advertising regardless of the legal basis of data processing.[64] If the respondent lodges an objection, personal data may no longer be processed for this purpose.[65]

5. CASE *META PLATFORMS AND OTHERS V. BUNDESKARTELLAMT*

Probably the most famous and most used social network today, Facebook, which is managed by the Meta concern, also provides an online advertising service and is thus financed. It is about targeted advertising that is adapted to individual users of the social network with regard to their consumer habits, interests, age, gender or some other personal characteristics, data about which is collected through cookies, text records that the terminal equipment of Internet users, in this case social network Facebook leaves you access to the specified network each time. The collected data enable the automated creation of detailed profiles of network users (profiling). In addition to the data that users directly provide during registration, the Meta concern also collects other data about said users and their devices, not only within Facebook but also outside of it, and then connects them to Meta's various user accounts. Insight into the huge amount of data collected in this way makes it possible to draw conclusions about the user's preferences and interests. The legal basis for this way of collecting user data was the usage contract with which users access the Facebook social network. Namely, when registering, which is necessary for using the Facebook social network, the user accepted the terms of use regarding the use of data and cookies. Meta has for years collected and processed data on user activities outside of Facebook, for example, visits to other websites and applications that are connected to Facebook, or owned by Meta, such as, for example, WhatsApp[66]. The German Federal Office for the Protection of Market Competition[67] in 2019 prohibited Meta from collecting and processing "off Facebook" data of Facebook users residing in the territory of the Federal Republic of Germany without consent. An adjustment of the general conditions of use was

---

63 Kramar, Kosta, *op.cit*., note 29, p. 20.

64 Mišćenić, E., *et al., Europsko privatno pravo - posebni dio*, Školska knjiga, Zagreb, 2021, p. 321.

65 Art. 21, par.3. GDPR.

66 Case C-252/21 Meta Platforms *et al.*. (general terms of use of the social network) ECLI:EU:C:2023:537 7, paras. 27. and 28.

67 German Federal Office for the Protection of Market Competition (Bundeskartellamt), an independent higher federal authority, based in Bonn, assigned to the Federal Ministry for Economic Affairs and Climate Action. The authority's task is to protect competition in Germany.

also requested so that it clearly follows from them that the specified off Facebook data will not be collected, linked to the user's Facebook accounts or used without consent. The German Federal Office for the Protection of Market Competition considered that the user's consent is not valid if giving it is a condition of using the social network. Meta's data processing practice, according to the German Federal Office for the Protection of Market Competition, represents an abuse of the dominant position of the Meta concern in the market of online social networks. Meta's data processing practice, according to the German Federal Office for the Protection of Market Competition, represents an abuse of the dominant position of the Meta concern in the market of online social networks. Companies within the Meta concern filed a lawsuit with the German High Land Court in Dusseldorf, refuting the conclusions of the German Office for the Protection of Market Competition. The High Land Court has sent a request to the European Court of Justice for a preliminary ruling with a number of questions concerning the interpretation of the GDPR. Regarding the question whether the national competition protection authority can supervise the compliance of data processing with GDPR requirements, the European Court of Justice gave an affirmative answer, however, the decision of the competition protection authority is limited only to the needs of determining the abuse of a dominant position and imposing measures to stop this abuse in accordance with the rules of competition law.[68] Regarding the protection of personal data and Facebook's collection and processing practices, the Court of Justice of the European Union clarified that the fact that the user visits websites or uses applications in no way means that the user gives consent to the collection of a category of special data in the sense of the GDPR.[69] The same applies when the user enters data on these pages or in these applications or when he selects the options contained on these pages or these applications, unless s/he has previously expressly expressed his/her choice that the data relating to him be publicly available to an unlimited number of people.[70]. When it comes to non-sensitive data, the Court of Justice of the European Union examined whether the collection of data is covered by the justifications provided for by the GDPR, which enable their processing without the consent of the data subject. Such a practice can only be justified under the condition that data processing is objectively necessary.[71] Thus, the Court of Justice of the European Union made it clear in its judgment that the

---

68 Sudar, Kulčar, *op.cit*, note 47, para. 62.

69 Art. 9. GDPR: "The processing of personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership is prohibited, as well as the processing of genetic data, biometric data for the purpose of unique identification of an individual, data related to health or data about sex life or sexual orientation of the individual."

70 *Op.cit.*, note 47, par. 84.

71 *Op.cit.*, note 47, par. 125.

personalization of advertising financed by Facebook cannot justify the processing of data if there is no valid and voluntary consent of the subject.[72] Consortium Meta, in accordance with the judgment of the European Court, at the end of 2023 introduced a new subscription model in accordance with GDPR rules. So from October 2023, Facebook and Instagram users have the option to choose a paid version of the subscription or continue using Facebook for free on the condition that their personal data is used, as before, for personalized advertising created by profiling based on the habits of Facebook users. Shortly after the introduction of the new subscription model, the European Union of Consumers (BEUC), the umbrella association of consumer protection organizations at the European Union level, and the non-profit organization European Center for Digital Rights filed separate complaints with the European Commission, Consumer Protection Cooperation Network and with the Austrian data protection authority[73] dissatisfied with the actions of the Meta consortium. They believe that Meta's new subscription model is in violation of GDPR rules because the choice made by users cannot be considered free. Also, Meta is breaching EU consumer law by using unfair, deceptive and aggressive practices, including partially blocking consumers from using the services to force them to take a decision quickly, and providing misleading and incomplete information in the process.[74] In accordance with Article 7 of the GDPR, the processing of personal data is based on consent. Consent must be given freely and voluntarily. [75] When assessing the voluntariness of consent, it is taken into account whether the performance of the contract, including the provision of the service, is conditioned by consent for the processing of personal data that is not necessary for the performance of that contract.[76]

6. CONCLUSION

Today we live in a 'disclosure society' characterized by 'a new political and social condition of radical interpersonal relations and a new virtual transparency that is

---

72 *Op.cit.*, note 47, par. 154.

73 Austria: NOYB files complaint against Meta over 'pay or okay' subscription model, [https://www.dataguidance.com/news/austria-noyb-files-complaint-against-meta-over-pay-or], Accessed 14 February 2024.

74 Consumer groups file complaint against Meta's unfair pay-or-consent model [https://www.beuc.eu/press-releases/consumer-groups-file-complaint-against-metas-unfair-pay-or-consent-model] Accessed 14.02.2024.

75 Art. 7. par. 2. GDPR: „If the respondent gives consent in the form of a written statement that also refers to other issues, the request for consent must be presented in such a way that it can be clearly distinguished from other issues, in an understandable and easily accessible form using clear and simple language. Any part of such a statement that constitutes a violation of this Regulation is not binding."

76 Art. 7. par. 4. GDPR.

redesigning our social landscape and transforming the notion of privacy.[77] The increasingly rapid development of digital technologies and new possibilities for processing and using personal data are the reasons why more and more users are expressing concern about the privacy of their personal data. A special concern for the security and privacy of users' personal data arises when the widespread practice of collecting personal data of users of social networks for the purpose of profiling and behavioral advertising. However, as pointed out, in the user's behavior we can very easily see the 'so-called the privacy paradox, i.e. the discrepancy between the declared expression of a high concern for privacy and the simultaneous manifestation of behavior that shows lack of concern for privacy, especially on the Internet and social networks.[78] In an increasingly digitally interconnected world, social media platforms will continue to have a profound impact on the private and public lives of their users, wielding such a significant and complex species of "digital dominance".[79] The social network Facebook has 3 billion monthly users, while Instagram has 2 billion.[80] Meta current changes to its service in the EU which require Facebook and Instagram users to either consent to the processing of their data for advertising purposes by the company or pay in order not to be shown advertisements, is unfair and illegal. The millions of European users of Facebook and Instagram deserve far better than this. Meta is, allegedly, breaching EU consumer law by using unfair, deceptive and aggressive practices, including partially blocking consumers from using the services to force them to make a decision quickly, and provide misleading and incomplete information in the process. Consumer protection authorities in the EU should spring into action and force the tech giant to stop this practice. The company's approach also raises concerns regarding voluntary user consent according to GDPR rules.[81] In our opinion, a data protection friendly online environment in the context of data collection for profiling and targeting purposes, should consist of, at least, the available and easily accessible no data collection choice. Moreover, such an option should be made preselected. It should also be possible, we believe, to have this choice recorded,

---

77 Pavuna, A., *Paradoks privatnosti: empirijska provjera fenomena*, Politička misao, god. 56, no. 1, 2019., p. 154.

78 Pavuna., *op.cit*., note 59, p. 132.

79 Burton, O.; Ding, J. T., *Digital Dominance and Social Media Platforms: Are Competition Authorities Up to the Task?* International Review of Intellectual Property and Competition Law, Volume 54, pp. 527–572., 2023, p. 565.

80 Rodriguez, S., *Instagram surpasses 2 billion monthly users while powering through a year of turmoil*, [https://www.cnbc.com/2021/12/14/instagram-surpasses-2-billion-monthly-users.html], Accessed 3 February 2024.

81 Consumer groups file complaint against Meta's unfair pay-or-consent model, [https://www.beuc.eu/press-releases/consumer-groups-file-complaint-against-metas-unfair-pay-or-consent-model], Accessed 15 February 2024.

so that users do not need to repeat their choice selection every time they access the website. The majority of users online do not have the needed competence, or patience and enough time to understand data protection options to make the choice that would fit their preferred level of data protection online. If the law only provides broad principles about consent being informed and free, it will only continue to favor powerful data controllers, who rely on legal interpretations and technological solutions that only fit particular interests. In our opinion, more specific regulation in this particular field is required. Normative regulation of personal data protection will be more challenging with the development of artificial intelligence, which will set new technical frontiers and legal challenges and uncertainties. In that sense, development of the legal framework for personal data protection with implementation of the main legal principles for access, collection and personal data processing need to be adjusted to implementation of new AI technology solutions. The processing and analyzing of personal data, which will be powered by AI technological solutions, are becoming an additional legal challenge in the European regulation of personal data protection. The possibility of implementation AI technological solutions in collecting, processing and analyzing data are huge. That opens up the need for additional regulation of the personal data protection framework and appropriate implementation of the main principles for AI technological solutions, according to the risk based approach regulated by the Artificial Intelligence Act.

REFERENCES

BOOKS AND ARTICLES

1. Aliyev, I. A.; Rzayev, G. A.; Ibrahimova, A. N., *Artificial Intelligence and Personal Data: International and National Framework*, Peace Human Rights Governance, Vol. 5., No. 1., 2021., pp. 97–123.
2. Belanger, F.; Crossler, R. E., *Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems*, MIS Quarterly, Vol. 35., No. 4., 2011, pp. 1017–1041.
3. Bosco, F., *et al., Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and perspectives from European Data Protection Authorities*, in: Gutwirth, S.; Leenes, R.; de Hert, P., (eds.), Reforming European Data Protection Law, Springer International Publishing AG, 2015, p. 17
4. Brezak, M., *Pravo na osobnost*, *Pravna zaštita osobnih podataka od zlouporabe,* Zagreb, Nakladni zavod Matice Hrvatske, 1998
5. Burton, O.; Ding, J. T., *Digital Dominance and Social Media Platforms: Are Competition Authorities Up to the Task?* International Review of Intellectual Property and Competition Law, Vol. 54, 2023, p. 565

6. Custers, B., *et al., A comparison of data protection legislation and policies across the EU*, Computer Law & Security Review, Vol. 34, No. 2, 2018, pp. 234–243
7. Custers, B., *et al., Introduction*, in Custers, B., et al., EU Personal Data Protection in Policy and Practice, Information Technology and Law Series, vol 29. T.M.C. Asser Press, The Hague. 2019, Springer, pp. 1–16
8. Czerniawski, M., de Hert, P., Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context, International Dana Privacy Law, Vol. 6., No. 3., 2016, pp. 230–243
9. Čizmić, J.; Boban, M., *Učinak nove EU Uredbe 2016/679 (GDPR) na zaštitu osobnih podataka u Republici Hrvatskoj,* Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 39, br. 1, pp. 377-410, 2018, p. 382
10. Elvy, S. A., *Paying for Privacy and Personal Dana Economy*, Columbia Law Review, Vol. 117, No. 6., 2017, pp. 1369–1459
11. Fuster, G. G., *The emergence of personal data protection as a fundamental right of the EU*, Springer International Publishing Switzerland, 2014, pp. 185–204
12. Gumzej, N., *Uredba o zaštiti osobnih podataka*, 2017, Projekt "Novi hrvatski pravni sustav" Pravnog fakulteta Sveučilišta u Zagrebu, p. 2
13. Gumzej, N., *Challenges of the digital environment for personal data privacy and security*, Društvo i tehnologija 2014, p. 707
14. Hall, L. B.; Clapton, W., *Programming the machine: Gender, race, sexuality, AI, and the construction of credibility and deceit at the border*, Internet Policy Review, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 10, No. 4, 2021, pp. 1 – 23
15. Hallinan, D.; Friedewald, M.; McCarthy, P., *Citizens' perceptions of data protection and privacy in Europe,* Computer Law & Security Review, Vol. 28, No. 3., 2012, pp. 263–272
16. Humerick, M., *Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence Comments*, Santa Clara High Technology Law Journal, Vol. 34, No. 1., 2018, pp. 393–418
17. Kamara, I.; Kosta, E., *Do Not Track initiatives: regaining the lost user control*, International Data Privacy Law, vol. 6, Issue 4, 2016, p. 6
18. Kiss, A,; Szoke, G, L., *Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation*, Springer International Publishing AG, 2015, pp. 314 -315
19. Kulhari, S., *Builduing-Blocks of a Dana Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity*, Nomos Verlagsgesellschaft mbH, Baden-Baden, 2018, pp. 23–37
20. Mišćenić, E., *et al., Europsko privatno pravo - posebni dio,* Školska knjiga, Zagreb, 2021, p. 321
21. Pavuna, A., *Paradoks privatnosti: empirijska provjera fenomena*, Politička misao, god. 56, no. 1, 2019, p. 154
22. Roos, A., *5 Core Principles of Data Protection Law*, The Comparative and International Law Journal of Southern Africa, Vol. 30, No 1., 2006, pp. 102–130
23. Sudar, Kulčar, M., *Zaštita privatnosti i sigurnosti pohranjenih podataka s osvrtom na izravni (direktni) marketing*, Politička misao, vol. XLII, 2005., no. 4, p.105

24. Van Dijk, N. *et al., Right engineering? The redesign of privacy and personal data protection, International Review of Law*, Computers & Technology, Vol. 32, No. 2 – 3, 2018, 230–256
25. Walters, D., *Behavioral Marketing: Delivering Personalized Experiences at Scale*, New Jersey, 2015, p. 3
26. Westin, A., *Privacy and Freedom*, New York, Atheneum, 1970.
27. Žliobaitė, I.; Custers, B., *Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models*, Artificial Intelligence and Law, Vol. 24, No. 2, 2016, pp. 183–201

EU LAW

1. Council of Europe, Committee of Ministers (1973), Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector, 26 September 1973; Council of Europe, Committee of Ministers (1974), Resolution (74) 29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector, 20 September 1974
2. Council of Europe, Convention on the Protection of Individuals with Automatic Processing of Personal Data, CETS br. 108, 1981
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free flow of such data, OJ 1995 L 281
4. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of privacy in the field of electronic communications, SL 2002 L 201 (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and the Council of November 25, 2009 amending Directive 2002/22/EC on universal services and user rights with regard to electronic communications networks and services, Directive 2002/58/EC on the processing of personal data and protection of privacy in the electronic communications sector (further: Universal Services Directive) and Regulation (EC) no. 2006/2004 on cooperation between national authorities responsible for the implementation of laws on consumer protection, OJ 2009 L 337
5. European Union Charter of Fundamental Rights, Official Journal of the European Union, C 326
6. Handbook on European Data Protection Legislation, Luxembourg: Publications Office of the European Union, 2020, p. 26
7. Proposal for a regulation of the European Parliament and the Council on respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on privacy and electronic communications) (COM(2017) 10 final)
8. Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals in connection with the processing of personal data and on the free movement of such data and on the repeal of Directive 95/46/EC (further: Regulation GDPR), OJ L 119/1
9. United Nations (UN), Universal Declaration of Human Rights, December 10, 1948

LIST OF NATIONAL REGULATIONS

1. Electronic Communications Act, Official Gazette no. 76/22

COURT OF JUSTICE OF THE EUROPEAN UNION

1. Case C-252/21 *Meta Platforms et al. (general terms of use of the social network),* Judgment of the Court (Grand Chamber) of 4th July 2023
2. Joined Cases C-92/09 and C-93/02, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen, Judgment of the Court (Grand Chamber) of 9th November 2010*
3. Case C-582/14 *Breyer v Bundesrepublik Deutschland* ECLI:EU:C:2016:779
4. Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v. Planet49 GmbH*
5. Case C-131/12, Google Spain, ECLI:EU:C:2014:317

WEB REFERENCES

1. Austria: NOYB files complaint against Meta over 'pay or okay' subscription model, [https://www.dataguidance.com/news/austria-noyb-files-complaint-against-meta-over-pay-or] Accessed 14 February 2024
2. Consumer groups file complaint against Meta's unfair pay-or-consent model, [https://www.beuc.eu/press-releases/consumer-groups-file-complaint-against-metas-unfair-pay-or-consent-model] Accessed 15 February 2024
3. *A cookie guide for micro, small and medium-sized businesses*, Agency for the Protection of Personal Data (AZOP), 2022., p. 4. [https://azop.hr/wp-content/uploads/2022/01/Vodic-za-kolacice.pdf], Accessed 3 February 2024