Zbornik Instituta za kriminološka
i sociološka istraživanja
2022 / Vol. XLI / 2-3 / 89-100
Originalni naučni rad
Primljeno: 15. novembar 2022. godine
Prihvaćeno: 14. decembar 2022. godine
DOI: 10.47152/ziksi2022036
UDK: 342.738
316.32:004

ALGORITHMIC SOCIAL SORTING AND NEW LEGAL NARRATIVES ON DIGITAL PRIVACY

Ivana STEPANOVIĆ*

The use of algorithms for social sorting has imposed the need to challenge the traditional understanding of the private sphere as a sealed-off realm free from surveillance and outside intervention. The relationship between private and public has become dynamic and complex while the borderline between the two zones remains to be in a state of flux. The concept of digital privacy is related to the data doubles rather than physical bodies, and it is limited to partial control over personal data. The General Data Protection Regulation, along with the new legislations, namely, Artificial Intelligence Act and Digital Services Act offer a conceptualisation of digital privacy that recognises novel dataveillance practices that involve the collection, interpretation, use and misuse of biometric and behavioural data. This paper uses the method of conceptual analysis to investigate the new definitions of digital privacy that emerge from the corpus of legislative acts including GDPR, AIA and DSA and find out how they generate new legal narratives on privacy that recognise the dangers of echo chambers and algorithmic decision-making.

KEYWORDS: privacy / human rights / algorithms / surveillance / personal data

* Institute of Criminological and Sociological Research, Belgrade, Serbia and Institute of Advanced Studies Kőszeg, iASK, Kőszeg, Hungary. E-mail: ivana.stepanovic@iask.hu

1. INTRODUCTION

Algorithmic systems increasingly interfere with and guide the political, economic, and cultural spheres. Since they are powered by personal data, they use human behaviour online as a resource, but this process of data extraction and digital production is not yet thoroughly regulated by international law. Legal definitions of privacy enshrined in various legislative acts merely mirror the social transformations imposed by technology. Chronologically, they always come after these changes have already been normalised as law strives to regulate the use of technology *post-festum* but the new legal definitions are enabling the creation of new legal narratives on complex and protean concepts such as digital privacy.

General Data Protection Regulation (GDPR)[1] as one of the key legislations regulating digital privacy has systematically redefined the concept of privacy in the online sphere. According to this legislation, the right to protection of personal data is merely a partial ability of an individual to control what happens with his or her personal data. It replaces the idea of total concealment of data with a much weaker demand for the transparency of processing personal data (Stepanović, 2019). However, personal data remain to be the fuel that drives the economy and leaves humans vulnerable not only to hacking and sporadic infringements of privacy, but also to mass surveillance, totalitarian control, and social engineering. The 'post-mortem privacy' reduces an individual to a 'digital double' (Buitelaar, 2017, p. 129) that is operating through the streams of personal data about locations, activities, opinions, behaviour and even emotions. Digital privacy refers to data doubles that are resembling abstract assemblage-like conglomerates of information. However, these digital bodies are substantially related to physical bodies. Individual privacy has been irreversibly exposed through the process of algorithmic (re)production of data as AI interferes in all forms of bureaucracy that are associated with the state, integrates into all aspects of labour, and even becomes a crucial part of entertainment, social and private life. Following the introduction of the GDPR, the EU is now introducing two new legal documents, namely, the Artificial Intelligence Act (AIA)[2] and the Digital Services Act (DSA)[3] which should also be applied internationally in the attempt to regulate the realm of the internet and AI on a global scale.

I argue that the three legislative acts radically redefined the right to the protection of personal data and introduced a new concept of digital privacy. Rather than being taken as an isolated problem, protection of personal data is now being considered in the context of invasive digital surveillance that goes to the level of monitoring behaviour and collecting biometric data. As such, it is deeply connected to the right

[1] General Data Protection Regulation, April 27, 2016, eur-lex.europa.eu/legal-content/EN/TXT/? uri= CELEX%3A32016R0679
[2] Artificial Intelligence Act, April 21, 2021, eur-lex.europa.eu/legal-content/EN/TXT/? uri= CELEX:52021PC0206
[3] Digital Services Act, December 15, 2020, eur-lex.europa.eu/legal-content/EN/TXT/? uri= CELEX:52020PC0825

to private life as well as personal freedom, dignity and autonomy. Reading these new laws shows that they are also attempting to regulate data flows and data protection while minimising the negative impacts of algorithmic surveillance and social sorting. In this paper, DGPR, AIA and DSA were examined to pinpoint the new legal definitions on digital privacy. These definitions are important because they are shaping the new legal narratives and pave the way to the reconfigurations of private and public and consequently reorganisation of the power structures.

Given that the concept of digital privacy emerges from the use of information technologies, it is inevitably shaped by various online privacy policies and legislative documents that are regulating these technologies. Legislative acts that are intended to be applied internationally together form a basis for regulating the internet sphere and therefore reshaping our understanding of online privacy. Specifically, GDPR, as the already adopted regulation along with the DSA and AIA, that are yet to be adopted, together constitute the three crucial documents that are vital for understanding the complexity of the right to privacy in the digital age. These documents emphasise the devastating consequences of algorithmic surveillance that goes beyond the passive collection of data towards active intrusion into human behaviour and therefore poses threat to the integrity of individuals through their extended digital self. The blurred borderlines between online and offline, physical and digital or virtual and real implicate that the impact of algorithms on individuals expands beyond the seemingly isolated sphere of the internet (Solomon, 2022: 88). The process of merging physical and digital in general points towards the convergence of the physical and digital legal subject. Together, they constitute the same entity even though the digital world is underregulated despite the fact that "the very idea of Metaverse means an ever-growing share of our lives, labour, leisure" and that "the Metaverse will also render more acute many of the hard problems of digital existence today, such as digital rights, data security, misinformation and radicalisation…" (Ball, 2022: 17).

2. THE ALGORITHMIC SOCIAL SORTING AND THE WEAK CONCEPT OF PRIVACY

In law as well as in theory, the concept of privacy has traditionally been associated with the sphere of home, family, body, sexuality, and correspondence, however, today, it is most frequently discussed in the context of digital information (Bennett, 2010; Lyon, 2019). In the realm of the internet, data doubles are comprised of bulks of data extracted from correspondences, internet searches and other online activities. Digital privacy is therefore exclusively related to personal data and legal protection is limited to the control of visibility of these data. The concept of digital privacy as the ability to have certain control over personal data has been famously explicated by Daniel Solove and Alan Westin (Solove, 2008; Westin, 1967), but it has also been reinforced by the big tech companies such as Google and Facebook who were propagating this definition long before the EU adopted the GDPR. Namely, these tech giants have coined the term 'privacy settings' which is more than just a technical term because it describes the philosophy of the private/public divide as the

creators of these companies have envisaged it. In the online realm where everything is public, one can only have the possibility to create provisional barriers which are limiting the visibility of personal data. This means that whether something is private, or public depends on the context, and it is not predetermined, which is why the contextual approach to privacy is more appropriate to describe contemporary distinctions between private and public (Barkhuus, 2012; Nissenbaum, 2004; Selbst, 2013). Hardly anything that has previously been considered exclusively private has not been touched by online surveillance including private homes, bedrooms, diaries, and correspondence. With the collection of behavioural data through capturing eye movements, tone of voice, facial muscle movements and other information, digital surveillance goes to the level of the privacy of thoughts. Such extent of surveillance can be explained by the fact that the internet is undeniably perceived as a public network dotted with pockets of privacy. It is being used for everything from banking and shopping to education, therapy, entertainment, and private correspondence. Within this public realm, there are privatised spaces and private areas as well as public groups, communities, and hangout places.

Privacy settings are supporting the definition of digital privacy as control over data but the control itself depends on the context. It is in fact only partial control which fails to ensure full confidentiality and secrecy, and there are two key levels of privacy infringements within social media and other online platforms. On one level, someone may have control over what they are sharing with their online 'friends' or 'followers'. They can decide whether they will publish specific information online and make it visible to wider audiences, a limited number of people or even just themselves. Privacy settings, therefore, allow gradation of privacy rather than offering just two distinct categories which is implying that information can be either private or public. However, the second level of online privacy involves harvesting personal data and using it for machine learning, algorithmic social sorting, governmental control, or marketing purposes (Lyon, 2019, p. 65). It potentially has effects not only on privacy but on a broader spectrum of human rights and freedoms.

The GDPR as the first legislative act which attempts to regulate the privacy of data on an international level offers its own version of the contemporary definition of privacy as a fundamental right. It recognises that 'personal data' are a very broad category of information that can be related not just to identifiers such as name, an identification number or location data but also information related to the physical, physiological, genetic, mental, economic, cultural, or social identity[4]. Furthermore, it recognises the process of 'profiling' as a process that is different to 'processing' as it 'consists of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, location or movements'.[5] By acknowledging a broad spectrum of

[4] General Data Protection Regulation art. 4(1), April 27, 2016 eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[5] General Data Protection Regulation art. 4(4), April 27, 2016 eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

personal data and a type of information processing that is typical of algorithmic sorting, the GDPR elevates the legal definitions of privacy and surveillance. It means that there is no strict distinction between personal information that are relevant and those that are not because any information that is traceable to a specific individual can potentially be used for surveillance practices including algorithmic profiling. In other words, algorithms as new bureaucratic surveillance mechanisms are not passive databases but active controllers that categorise, interpret, rearrange, and re-produce personal data or generate additional information on individuals based on calculations and predictions that are being used for psychological profiling.

On the other hand, it can be argued that the GDPR fails to capture one of the main challenges of protecting human rights with regard to the processing of personal data by offering a consent-based approach to the protection of privacy. Namely, the GDPR proposes that there is no infringement of privacy if someone gives consent to the processing of their personal data freely, provided that all other conditions are met, including the clarity of the consent form. However, in practice, this consent-based approach is proven to deliver partial results and there are certain restraints which should be taken into consideration. Given that the functioning of algorithms is not transparent and that 'data subjects' are not aware of the consequences of processing and profiling, it is questionable whether a 'freely given' consent is enough to protect one's privacy. The fact that 'digital platforms and services utilise big data analyses, predictive analysis, algorithms, and machine learning to produce (personal) information about individuals' (Mai, 2019, p. 113), it can be argued that human rights are being violated even with consent. To willingly accept the consequences of the processing of personal data, one has to have a very high level of digital literacy and be able to understand the complex mechanisms of privacy protection online (Baruh & Popescu, 2015; Moll & Pieschl, 2016) or be able to predict the ramifications of algorithmic profiling.

Shoshana Zuboff asks whether privacy policies in fact are 'surveillance policies' given that profit-driven platforms that collect personal data to create revenue are the core of 'surveillance capitalism' (Zuboff, 2019, p. 5). It can be argued that contemporary communication technologies are conceived as intricate monitoring systems with incredible capacities to collect, store and process all kinds of data which essentially makes them surveillance machines. They are using the same logic as traditional bureaucratic monitoring systems, and the only crucial difference is the increase in surveillance capacities (Dandeker, 2007, p. 39). As a result, surveillance is deeply embedded into these technologies and therefore incorporated into everyday lives, making the entire traditional sphere of privacy transparent via smart technologies that enable any gadget to be connected to the internet and source personal data. One of the major changes is the emergence of miniaturised and granulated surveillance which involves the collection of fleeting ephemeral data such as facial gestures, the amount of time someone spends watching a video etc. By expanding the scope of data, increasing the amount of information and artificial intelligence which can make sense of large bulks of data, surveillance processes are no longer just passive observation and classification, but active processes which are interpreting behaviour and modifying it (Zuboff, 2019, p. 19).

Considering the miniaturisation of surveillance that involves algorithmic profiling associated with manipulation, the GDPR, the DSA and AIA have been created to offer a more holistic approach to safeguarding fundamental rights in the age of AI and online platforms. Together they create a three-pillared fundament for the protection of human rights in the online realm not just within the EU, but also on a global level. These laws are aiming to set global standards which companies across the world need to respect if they want to survive in the market. They also offer a radically new articulation of the concept of privacy as they tend to merge different rights together with the aim to offer a comprehensive approach to online safety. While leaving the question of whether these legislative acts are capable of truly protecting individual rights in the digital age open, this paper remains focused on the exploration of narratives on privacy which emerge from them.

3. NEW LEGAL NARRATIVES ON THE INTERLINKED THREATS TO THE DIGITAL SELF

The GDPR is focusing on the protection of 'natural persons with regard to the processing of personal data and on the free movement of such data'[6]. It aims to protect the right to the protection of personal data in accordance with Article 8(1) of the Charter of Fundamental Rights of the European Union[7] and Article 16(1) of the Treaty on the Functioning of the European Union[8], while at the same time striving to 'contribute' to 'freedom, security and justice' as well as 'the well-being of natural persons'.[9] The key innovations to the protection of personal data are the concepts of transparency, consent and the right to access and erase data or 'to be forgotten'. However, this legislation has been extensively criticised for failing to allow users more control over their personal data. Most notably, it has been emphasised that the GDPR faces the so called 'pacing problem' because it is based on 'ex post control' and only 'scratches the surface' of privacy infringement issues due to the neck-breaking speed of sharing, producing, and manipulating of information with new technologies (Renda, 2021, p. 5). Furthermore, the concept of consent has been criticised for allowing individuals to give consent to manipulative practices which are often 'hidden' (Hacker, 2021, p. 17). The GDPR, on the other hand, recognises the issue of 'profiling' of data which is different from the simple 'processing' of data. Automated individual decision-making, including profiling, is regulated by article 22, but it has been criticised for being overly vague, particularly because many activities which could be qualified as profiling could fall out of the scope of Article 22 and because

[6] General Data Protection Regulation, April 27, 2016, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[7] Charter of Fundamental Rights of the European Union art. 8(1), October 26, 2012, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT

[8] Treaty on the Functioning of the European Union art. 16(1), October 26, 2012, eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_2&format=PDF

[9] General Data Protection Regulation, April 27, 2016 eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

the concept of 'automated decision' is not clarified enough (Gil Gonzales & de Hert, 2019, p. 597).

The GDPR recognises the problem of profilrendaing and considers automatic processing related to algorithmic sorting. This profiling is not always reduced to passive surveillance as it may involve interventions into human behaviour such as in the case of the Cambridge Analytica scandal which involved the psychological profiling and manipulation (Risso, 2018, p. 71; Spencer, 2020, p. 960). However, GDPR does not fully anticipate all the consequences of algorithmic processing of data, especially implications on identity and private life or social, economic, and other discriminatory practices that may stem from algorithmic profiling (Wachter, 2018, p. 436) which include interlinked and intertwined infringements of different human rights and freedoms.

But while the GDPR focuses on the protection of personal data, AIA and DSA further develop the mechanisms for the protection against the grave consequences of algorithmic profiling. Currently in the form of a proposal, both legislative acts wacwere created by the EU with the aim to get the same international recognition as the GDPR. Both proposals start with an 'explanatory memorandum' text which explicates reasons and objectives for introducing such laws. The DSA proposal which has been created in 2020 is a response to 'innovative information society (digital) services' which are changing daily lives and 'transforming the way they communicate, connect, consume, and do business'[10]. Similarly, the AIA proposed in 2021 is a response to the exacerbated use of algorithms across different sectors with the aim to create a legal framework for the lawful and ethical use of AI considering both positive and negative consequences of such technologies.

The two new proposed legislative acts aim to regulate different areas of the digital realm, but together they are also further developing the concept of online privacy. They are going beyond the GDPR, offering stronger protection of individual rights while at the same time fostering technological progress. Reading these legal texts shows that the right to privacy is always related to other human rights and freedoms. Both legislative acts call for respecting fundamental rights to maximise online safety. The protection of private data is therefore firmly connected to a myriad of other rights. The new legal narratives this legislation is anticipating are already visible in the explanatory Memorandum of the AIA. It states that the use of AI can 'adversely affect a number of fundamental rights enshrined in the EU Charter of Fundamental Rights' and that this legislation 'seeks to ensure a high level of protection for those fundamental rights and aims to address various sources of risks through a clearly defined risk-based approach'. More specifically, it is written that this act has the goal to protect the right to human dignity, respect for private life and protection of data while also ensuring non-discrimination and equality between women and men and prevent the negative effects on rights to freedom of expression, freedom of assembly, the right to an effective remedy and a fair trial, the rights of defence and the

[10] Digital Services Act, December 15, 2020, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0825

presumption of innocence, workers' rights to fair and just working conditions, the rights of the child, integration of persons with disabilities, environmental protection as well as health, safety and consumer protection[11].

The DSA also strives to defend interlinked fundamental rights while recognising the need to develop appropriate risk management tools which would prevent the use of 'manipulative techniques'[12]. In the Explanatory Memorandum, it is underlined that the protection of the freedom of expression is crucial, along with the right to an effective remedy, non-discrimination, the rights of the child, human dignity, protection of personal data and privacy online. There is a special emphasis on the protection of privacy on the internet as it introduces prohibitions which are supposed to 'limit incentives for online surveillance'. The DSA also has the aim to enhance cross-border cooperation, complement the European Democracy Action Plan[13] and contribute to 'building more resilient democracies'[14].

Even though AIA and DSA bring about many innovations and recognise some of the problems in the online world, they still contain many loopholes and inconsistencies which could lead to problems with the implementation. Regarding privacy protection, there are several problems which need to be addressed. Even though the proposal of AIA underlines the importance of protecting fundamental rights, the legislation does not provide remedies to protect individuals against AI decision-making, nor does it contain a clause on compliance with GDPR which is focusing more narrowly on the protection of personal data (Ebers et al., 2021, p. 600). Furthermore, the proposed legislation has been criticised for offering a narrow definition of manipulation (Veale & Zuiderveen Borgesius, 2021, p. 4).

The DSA 'raises the transparency bar higher' to battle against manipulative practices related to algorithmic profiling and social sorting but it will most likely not prevent either manipulation or 'mind-reading' practices because informed consent requires very advanced knowledge and digital literacy, and not all the coneberssumers will give up the convenience to avoid unethical practices (Hacker, 2021, p. 29). Additionally, it is worth noting that this legislation is targeting mainly large platforms while failing to protect individuals from harm caused by smaller ones.

Even though it is questionable how efficient will these two proposed legislative acts be in preventing the harms of algorithmic social sorting, it is undeniable that they introduce new narratives about privacy by acknowledging various unethical practices associated with surveillance and AI. It is also evident that they will

[11] Artificial Intelligence Act, April 21, 2021, eur-lex.europa.eu/legal-content/EN/TXT/? uri= CELEX:52021PC0206

[12] Digital Services Act, December 15, 2020, eur-lex.europa.eu/legal-content/EN/TXT/? uri= CELEX:52020PC0825

[13] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan, December 3, 2020, eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM% 3A2020%3A 790%3AFIN

[14] Digital Services Act, December 15, 2020, eur-lex.europa.eu/legal-content/EN/TXT/?uri= CELEX:52020PC0825

encourage greater cross-border cooperation by putting emphasis on democratic values in the online realm. Just like GDPR caused a domino effect outside the EU, it is highly likely that AIA and DSA will influence the rest of the world and impose new rules around safety on the internet with online privacy at the very centre.

The main novelty that the three legislative acts bring about is the recognition of the risks associated with algorithms, predictive analytics, 'pervasive connectivity' and 'data-driven business models' (Gawer, 2022: 122). In other words, they emphasise that the "Artificial Intelligence (AI)-based surveillance technologies such as facial recognition, emotion recognition and other biometric technologies have been rapidly introduced by both public and private entities all around the world, raising major concerns about their impact on fundamental rights, the rule of law and democracy" (Gawer, 2022: 147). Even though all three legislative acts are widely criticised for the loopholes (Raposo, 2022: 88), they are nevertheless revolutionary as they together offer a holistic approach to limiting the negative impacts of algorithmic profiling, changing the global standards for the protection of digital privacy and offering new narratives that are potentially transforming the definitions of the private/public dichotomy which could be transcending the European borders and being accepted internationally. Placing the focus on the protection of individuals and collectives against algorithmic surveillance reinstates the importance of (digital) privacy as one of the key pillars of contemporary democracies.

4. CONCLUSION

Digital surveillance which has been transformed from the passive collection of information into the active (re)production of personal data has challenged the existing theoretical, legal, and everyday definitions of privacy. The private/public divide has been relativised and contextualised which has resulted in the adoption of a very weak concept of privacy defined as the right to have partial control over the inevitable processes of sharing and processing of personal data. This minimalistic notion of privacy justified the logic of surveillance capitalism, but it seems that a new legal concept of privacy started to emerge as a response to multiple problems that are stemming from the practices of data surveillance and algorithmic social sorting.

The General Data Protection Regulation, along with the proposed Artificial Intelligence Act and Digital Services Act have been created with the aim to offer more comprehensive protection of privacy as a part of a network of fundamental rights and therefore create a safer online space not just within the EU but also worldwide. These legislative acts recognise that misuse of personal data can have a profound negative impact on individuals and therefore humanity as a whole. The ramifications are going beyond the privacy of data and spreading to the privacy of thoughts, emotions and physical bodies which can lead to different types of manipulation, discriminatory practices, and infringements of a whole spectrum of human rights and freedoms. Privacy is therefore placed at the very centre of the wider problem of protecting the individual in the online realm.

This research has shown that the GDPR as well as the new proposed new legislative acts offer new definitions of online privacy and safety while putting the protection of personal data in a larger context of interlinked human rights and freedoms. AIA and DSA acknowledged that processing personal data and algorithmic profiling can lead to a variety of discriminatory and biased practices while enclosing users inside echo chambers, jeopardising the presumption of innocence or the right to a fair trial. From the legal perspective, it is questionable whether AIA and DSA can truly safeguard individual rights in the age of big data and artificial intelligence systems with the so-called 'balanced approach' and multiple problems and loopholes. However, they inevitably contribute to a major shift in understanding privacy in the information age.

REFERENCES:

(1) Artificial Intelligence Act, April 21, 2021, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206
(2) Ball, M. (2022). *The Metaverse: And How It Will Revolutionize Everything*. New York: Liverlight Publishing Corporation
(3) Barkane, I. (2022). Questioning the EU Proposal for an Artificial Intelligence Act: The need for prohibition and a stricter approach to biometric surveillance. *Information Polity, 27*(2), 147-162. https://doi.org/10.3222/IP-229012
(4) Barkhuus, L. (2012). The Mismeasurement of Privacy: Using Contextual Integrity to Reconsider Privacy. *HCI. CHI'12: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (*pp. 367-376). https://doi.org/10.1145/2207676.2207727
(5) Baruh, L., & Popescu. M. (2015). Big Data Analytics and the Limits of Privacy Self-Management. *New Media & Society, 19*(4), 579-596. https://doi.org/10.1177/1461444815614001
(6) Bennett, C.J. (2010). In Defence of Privacy: The Concept and the Regime. *Surveillance & Society, 8*(4). https://doi.org/10.24908/ss.v8i4.4184
(7) Buitelaar, J.C. (2017). Post-mortem privacy and informational self-determination. *Ethics and Information Technology, 19*, 129–142. https://doi.org/10.1007/s10676-017-9421-9
(8) Charter of Fundamental Rights of the European Union, October 26, 2012, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT
(9) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan, December 3, 2020, eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A790%3AFIN
(10) Dandeker, C. (2007). Surveillance: Basic Concepts and Dimensions. In: S. Hean & J. Greenberg (Eds.), *The Surveillance Studies Reader* (pp. 39-52). Maidenhead: McGraw-Hill Education.
(11) Digital Services Act, December 15, 2020, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0825
(12) Ebers, M., Hoch, V.R.S., Rosenkranz, F., Ruchemeier, H., & Steinrötter, B. (2021). The European Commission's Proposal for an Artificial Intelligence Act – A Critical Assessment by Members of the Robotics and AI Law Society (RAILS). *Multidisciplinary Scientific Journal, 4*, 598-603.

(13) Gawer, A (2022). Digital platforms and ecosystems: remarks on the dominant organisational forms of the digital age. *Innovation, 24*(1), 110-124. https://doi.org/10.1080/14479338.2021.1965888
(14) General Data Protection Regulation, April 27, 2016, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
(15) Gil Gonzalez, E., & de Hert, P. (2019). Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles. *ERA Forum, 2019*(4), 597–621. https://doi.org/10.1007/s12027-018-0546-z
(16) Hacker, P. (2021). Manipulation by Algorithms. Exploring the Triangle of Unfair Commercial Practice, Data Protection, and Privacy Law. *European Law Journal,* https://doi.org/10.1111/eulj.12389
(17) Lyon, D. (2019). Surveillance Capitalism, Surveillance Culture and Data Politics. In: D. Bigo, E. Isin & E. Ruppert (Eds.), *Data Politics: Worlds, Subjects, Rights* (pp. 64-79). London and New York: Routledge.
(18) Mai, J. (2019). Situating Personal Information: Privacy in the Algorithmic Age. In: R. F. Jørgensen (Ed.), *Human Rights in the Age of Platforms*. Cambridge, Massachusetts: The MIT Press.
(19) Moll R., & Pieschl S. (2016). Expecting Collective Privacy: A New Perspective on Trust in Online Communication. In: B. Blöbaum (Ed.) *Trust and Communication in a Digitized World* (pp. 239-251). Progress in IS book series. Cham: Springer. https://doi.org/10.1007/978-3-319-28059-2_14
(20) Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review, 79*, 119-158.
(21) Raposo, V. L. (2022) Ex machina: preliminary critical assessment of the European Draft Act on artificial intelligence. *International Journal of Law and Information Technology*, 30(1), 88-109. https://doi.org/10.1093/ijlit/eaac007
(22) Renda, A. (2021). Making the Digital Economy: 'Fit for Europe'. *European Law Journal*. https://doi.org/10.1111/eulj.12388
(23) Risso, L. (2018). Harvesting Your Soul? Cambridge Analytica and Brexit. In: C. Jansohn (Ed.), *Brexit Means Brexit*. Mainz: Academy of Sciences and Literature.
(24) Selbst, A. D. (2013). Contextual expectations of privacy. *Cardozo L. Rev., 35*, 643.
(25) Solomon, M. R. (2022). Digital Identity: The Postmodern Consumer Chameleon. In: R. Llamas & B. Russel (Eds.), *The Routledge Handbook of Digital Consumption*. London and New York: Routledge
(26) Solove, D. (2008). *Understanding Privacy*. Cambridge: Harvard University Press
(27) Spencer, S. B. (2020). The Problem of Online Manipulation. *University of Illinois Law Review*, 2020(3), 960-1000. http://dx.doi.org/10.2139/ssrn.3341653
(28) Stepanović, I. (2019). Privacy and Digital Literacy: Who is Responsible for the Protection of Personal Data in Serbia? *Zbornik Instituta za kriminološka i sociološka istraživanja, 38*(3), 45-56.
(29) Treaty on the Functioning of the European Union art. 16(1), October 26, 2012, eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_2&format=PDF
(30) Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International, 22*(4), 97-112. https://doi/10.9785/cri-2021-220402/html
(31) Wachter, S. (2018). Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination and the GDPR. *Computer Law & Security Review, 34*(3), 436-449.
(32) Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum

(33) Zuboff, S. (2019). We Make Them Dance: Surveillance Capitalism, the Rise of Instrumentarian Power, and the Threat to Human Rights. In: R.F. Jørgensen (Ed.), *Human Rights in the Age of Platforms.* Cambridge, Massachusetts: The MIT Press

ALGORITAMSKO SORTIRANJE I NOVI PRAVNI NARATIVI O DIGITALNOJ PRIVATNOSTI

Korišćenje algoritama za društveno sortiranje nametnulo je potrebu da se preispita tradicionalno definisanje privatne sfere kao odvojene sfere pošteđene nadzora i spoljašnje intervencije. Odnos između privatnog i javnog je postao dinamičan i kompleksan dok je linija podele između te dve sfere u stanju pokreta. Opšta uredba o zaštiti podataka zajedno sa dve nove directive, naime, Uredba o veštačkoj inteligenciji i Uredba o digitalnim uslugama konceptualizuje digitalnu privatnost spram novih praksi nadzora koje uključuju prikupljanje, interpretaciju, korišćenje i zloupotrebu biometrijskih i bihejvioralnih podataka. Ove uredbe pozicioniraju parvo na zaštitu privatnih podataka unutar šireg konteksta privatnosti, ljudskog dostojanstva, slobode govora i drugih osnovnih prava i sloboda prepoznajući opasnosti algoritamskog nadzora. Ovaj rad koristi medodu konceptualne analize da istraži nove narative o digitalnoj privatnosti koji proističu iz korpusa pravnih akata Evropske Unije koji čine Opšta uredba o zaštiti podataka, Uredba o veštačkoj inteligenciji i Uredba o digitalnim uslugama.

KLJUČNE REČI: privatnost / ljudska prava / algoritmi / nadzor / lični podaci