Zbornik Instituta za kriminološka
i sociološka istraživanja
2019 / Vol. XXXVIII / 3 / 45-56
Originalni naučni rad
Primljeno: 29. novembra 2019. god.
UDK: 342.738(497.11)

PRIVACY AND DIGITAL LITERACY: WHO IS RESPONSIBLE FOR THE PROTECTION OF PERSONAL DATA IN SERBIA?*

Ivana Stepanović*
Institute for Criminological and Sociological Research, Belgrade

While privacy laws fail to fully protect personal data in a digital form, especially considering capacities for storing them and the speed of sharing and multiplying them, individuals are responsible to safeguard their privacy online and take steps to prevent abuse. However, this requires technical skills and digital literacy which entails up-to-date knowledge on digital privacy protection and use of a whole set of devices, software, browser extensions and encryption techniques. The General Data Protection Regulation is an attempt to redeem control over privacy protection and divide responsibility between users and other subjects such as data controllers, data processors and other authorities. However, in countries outside the EU where citizens are not protected by the GDPR, the emphasis is much more on individual responsibility. The aim of this paper is to stress out the importance of dividing responsibility for privacy protection among different actors in Serbia.

KEYWORDS: privacy / personal data / digital literacy / digital identities / GDPR

* This paper is a result of research Project "Crime in Serbia: phenomenology, risks and the possibilities of social intervention" (47011), financed by the Ministry of Education, Science and Technological Development of Republic of Serbia.
* E-mail: ivana.stepanovic@gmail.com

INTRODUCTION

Data protection has become a crucial aspect of privacy protection in general. In fact, privacy today is often reduced to the privacy of data both on the level of theory and in the realm of law because an individual itself is often reduced to data (Lyon, 2010: 325). Due to the prevalence of smartphones, social networks, cloud servers and big data, protecting "data relating to an identifiable individual" is the key element of protecting one's privacy in the contemporary world (Politou, et al 2018). Personal data is a concept that encompasses not just names, addresses, identification numbers and passport numbers, but also all data that can be traced back to an individual including photos, browsing history, profiles on social networks, online activity and anything that leaves a digital trace. All of these traces collectively constitute "digital doubles" that are transparent and traceable on the internet (Haggerty, Eriscon, 2000: 605).

Ubiquitous technologies capable of collecting huge amounts of personal data, tracking locations and monitoring activities are therefore perceived as surveillance technologies. They allow identifying, monitoring and tracking digital doubles due to unconstrained ability to collect, share, duplicate and reuse personal data. Moreover, the internet of things makes these surveillance technologies deeply embedded into personal lives (Schaar, 2009: 46), invading private as well as public spaces (Moreham, 2006; Nissenbaum, 1998) and leaving individuals entangled in complex surveillance networks (Gilliom, Monahan, 2013: vii). This is why claims about "surveillance society" (Lyon, 1994; Murakami Wood, 2009; Fuchs, 2010; Gilliom, Monahan, 2013) and "post-privacy era" (Meyrowitz, 2002; Heller, 2011; Schaar, 2009; Schramm, 2012) are so prevalent. However, it can also be argued that privacy is not an abandoned concept but a notion that has been transformed and redefined to adjust itself to the logic of big data. Rather than understanding privacy in the sense of concealment of information that is considered as private, it should be perceived as an ability to have "more control and transparency" on the way personal data is being used and reused (Politou et al 2018).

Due to the intricate mechanisms for privacy protection online and data protection strategies that involve using a whole set of technologies and understanding how they function, individuals are forced to rely on their online privacy literacy to protect their data. This new literacy refers to knowledge that is far more complex than reading and calculating, but also entails the ability to understand and control personal data on the internet (Pangrazio, Selwyn, 2018). The responsibility is therefore shifted to the individual who is disempowered as communication technologies come with significant limitations regarding privacy protection.

In the EU, the General Data Protection Regulation is an attempt to redeem control and transparency regarding the processing of data, but also an attempt to divide responsibility for privacy protection among different actors. Despite currently existing technical problems with implementing certain principles of the GDPR such as consent withdrawal and the right to be forgotten (Politou et al 2018), this legislation has created a framework for effective protection of personal data giving

individuals more control over their privacy. In Serbia, Data Protection Law is created to meet the EU standards and comply with the GDPR, but the law fails to cover some aspects of data protection and its implementation which was supposed to start on August 2019 is still uncertain because many subjects who should be bound by this law are not ready to start implementing it[1]. In countries such as Serbia which are not in the EU and are not protected by the GDPR, individuals feel that they are much more responsible for their privacy and data protection and are forced to rely on their digital literacy as they cannot count on the protection by the subjects who are collecting and processing their data. In the second chapter, I will analyse the modern and redefined notion of literacy which includes digital literacy and knowledge about online data protection. In the third chapter, I will discuss the GDPR's division of responsibilities among different actors and analyse the impact of this division on individual privacy. In the fourth chapter, I will discuss the issue of individual and collective responsibility for data protection in Serbia, map the problematic areas and stress out the importance of sharing responsibilities among different actors involved in storing and processing of personal data.

1. DIGITAL LITERACY IN THE CONTEXT OF PRIVACY PROTECTION

Digital literacy is a new type of literacy which has emerged with new digital technologies and it means that being literate no longer entails only the basic skills such as reading, writing and calculating, but also knowledge and understanding of complex systems (Pieschl, Moll, 2016, Baker, 2010). Digital literacy means not only knowing how to use digital technologies in everyday life but also knowing how to use them efficiently, responsibly and productively. This means that technology has altered the very nature of literacy (Kuzmanović, 2017) and it is now becoming increasingly more intricate and difficult to grasp. Since digital technologies keep evolving very fast introducing new features and daily updates, being digitally literate means being able to adjust to new changes and constantly update knowledge.

The need for improving digital literacy worldwide has been emphasised after the 2016 presidential election in the US when the Cambridge Analytica scandal has shown that consequences of poor digital literacy can lead to aggravating consequences such as mass manipulation of voters (Breakstone at al. 2018). Some authors have pointed out that digital transformation should be accompanied by the development of digital skills and even introducing an internationally accepted digital literacy index (Krish et al. 2018), while others have emphasised the importance of "media literacy" in the digital era and "post-truth era" (Friesem, 2019). In Serbia, standards for the development of digital competence are defined only on a basic

[1] Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti https://www.poverenik.rs/ (Accessed: 05.09.2019)

level and there are not many pieces of research that could assess the level of digital literacy in this country (Kuzmanović, 2017).

Digital literacy is crucial for everything one does online including researching information, filtering information, fact-checking, communicating and protecting privacy by safeguarding personal data (Pieschl, Moll, 2016; Kuzmanović, 2017). It can even be claimed that the "capacity to understand and control one's personal data is now a crucial part of living in contemporary society" (Pangrazio, Selwyn, 2018). However, privacy protection online requires using a whole set of strategies, understanding multifaceted systems of encryption, knowledge on various privacy settings available across different platforms or electronic devices, reading and understanding of various privacy policies and capability of grasping complex information systems. This means that it is virtually impossible to have any kind of privacy online without digital literacy, and yet digital literacy requires advanced knowledge in different fields (Moll and Pieschl, 2016: 239).

Even if we narrow down digital literacy to data literacy, it is still spread across different fields of knowledge. Some authors have tried to define "online privacy literacy" by specifying its different aspects such as knowledge about practices of organisations, institutions as well as online service providers, knowledge about technical aspects of data protection, knowledge about the legal framework in a specific country and understanding of user strategies for protecting individual privacy (Trepte, at al. 2014). However, as defined in this way, online privacy requires persistent efforts of individuals to take care of their personal data. This is essentially an aspect of neoliberal governmentality which is not confined to the repression of individual's freedom but also promotes individual's responsibility for their own self and increasing of their "intellectual capacities" (Rose, 1991: 4). Privacy is something so inherent to the self, that its protection requires specific knowledge about individual rights as well as technological possibilities for protecting personal data. As neoliberalism supports an ethics of individual autonomy and individual responsibility (Wrenn, Waller, 2017), the neoliberal subject is held responsible for its knowledge about dimensions of the right to privacy which is an aspect of the self.

But paradoxically, even though the internet is (or should be) available to everyone, not everyone has the same control over their privacy online as individuals are limited by their knowledge and digital literacy as well as technologies themselves and their built-in mechanisms for privacy protection and data sharing. Namely, modern technology offers only limited options for privacy protection that are only partially safeguarding personal data, while the logic of big data is undermining the whole concept of individual privacy on the internet. As a result, efforts to protect privacy despite these limitations are deemed as futile even with individuals who are digitally literate (Baruh, Popescu, 2015: 597).

On the one hand, individuals are faced with the responsibility to protect their privacy and there is a growing demand for developing strategies for education on privacy literacy. Some recent research projects have shown that persons with high-level privacy literacy have privacy concerns and lack of trust towards data-driven companies (Rosenthal et al. 2019) which is why they feel that protection of personal

data is their responsibility, especially on social media. However, due to the "increasing difficulty in managing one's online personal data", there is a feeling of a loss of control which is also known as "privacy fatigue" at the same time, as some existing researches suggest (Choi, Park, Jung, 2017). This is why individuals feel as if they are forced to use digital technologies that are invading their privacy in order to work, play, communicate and maintain their personal relationships while the duty to protect their privacy online seems like a daunting task.

Can privacy simply be a responsibility of an individual alone, or should the responsibility be shifted to other actors as well? As some suggest, it can be argued that privacy is itself a prerequisite for responsibility as "one cannot assume responsibility for something without first articulating what it is that one is assuming responsibility for, and the right to privacy protects the 'drafting space' in which to articulate it" (Hajdin, 2018). And if this is the case, then protecting privacy should be enabled and provided for the individual by a certain authority. And even if an individual is partially responsible for protecting his/her privacy, there is a need to divide responsibility in such a way to include different actors involved in collecting and processing personal data. This is due to the very nature of online platforms which, given that they often offer user-generated content (this is the case for the social media and other platforms), require a "dynamic interaction between platforms, users and public institutions" rather than allocating responsibility to only one central actor (Helberg, Pierson, Poell, 2017). Hence, privacy protection does not necessarily need to be a burden for an individual alone who has to master online privacy literacy, but it can be perceived as a shared responsibility of different actors.

2. GDPR: INDIVIDUAL VS COLLECTIVE RESPONSIBILITY

The General Data Protection Regulation (GDPR)[2] has transformed the way privacy is understood today in the context of online data protection. Its primary goal is to protect the human right to privacy and ensure respect of private and family life, communication and personal data (Prlja, 2018: 92). It stipulates that personal data should be processed "lawfully, fairly and in a transparent manner in relation to the data subject"[3]. Furthermore, this regulation specifies that there should be an explicit and legitimate purpose for data processing (purpose limitation), that data collected and processed should be adequate, relevant and limited (the principle of data minimisation), that the data should be accurate and kept up to date (accuracy), kept no longer than necessary for the specific purpose (storage limitation) and processed in such a way that personal data are secured and protected (integrity and confidentiality) while the controller is responsible for compliance with this regulation (accountability)[4].

[2] General Data Protection Regulation https://gdpr-info.eu/ (Accessed: 21.08.2019.)
[3] General Data Protection Regulation, Article 5 https://gdpr-info.eu/art-5-gdpr/ (Accessed: 21.08.2019)
[4] Ibid.

The GDPR is a document which makes the first step towards regulating data privacy on a global level as it is the first regulation that sets standards for protecting privacy worldwide. Since it is applicable within the EU, it is designed to regulate all segments of the internet that affect EU citizens and therefore already has an impact across global platforms and institutions that are processing personal data of residents of the EU countries. Its key postulates about privacy are therefore affecting the whole world. The GDPR defines privacy as the right to have control over personal data. Starting from the premise that collecting and processing data for various purposes is inevitable and that the right to privacy in the age of big data can no longer be the right to total anonymity or the right to concealment of data. The concept of ideal privacy may be lost in a certain way, but this document tries to redeem the right to privacy of data by giving more control to individuals. This is only achievable by defining roles and dividing responsibilities.

According to the GDPR, privacy protection is the responsibility of a number of actors. The individual or the ‘data subject’ is responsible to respect the principle of consent as stipulated in article 7 of the GDPR[5]. This means that the data subject can give its consent to the controller of the information to processing of his or her personal data, but can also withdraw this consent at any time. However, a data subject has to be clearly informed about the processing of personal data and the request for consent should be "presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language"[6]. This means that an authority who collects and processes data also shares responsibility with an individual who is referred to as data subject.

Responsibility is therefore shared between different actors: data subject, controller, processor, third party, data protection officer and supervisory authority. It is important to distinguish these actors and their roles but, most importantly, understand their responsibilities. While ‘controller’ is a "natural or legal person, public authority, agency or another body which determines purposes and means of the processing of personal data", the ‘processor’ is a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"[7]. According to Article 4, the data controller is considered to be "the principal party for responsibilities such as collecting consent, managing consent-revoking, enabling right to access, etc."[8]. This means that the data controller has more responsibilities than the data processor who only works on their behalf. Additionally, a third party is a subject authorised to process personal data by either controller or processor.

[5] General Data Protection Regulation, Article 7 https://gdpr-info.eu/art-7-gdpr/ (Accessed: 21.08.2019)
[6] Ibid.
[7] General Data Protection Regulation, Article 4, https://gdpr-info.eu/art-4-gdpr/ (Accessed: 21.08.2019)
[8] GDPR EU https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/ (Accessed: 21.08.2019)

Data subjects, data controllers, data processors and third parties are subjects who directly interact with personal data. But to ensure compliance with the GDPR, this regulation introduces authorities responsible for overseeing data protection. Data protection officer is an authority within a company that processes the personal data of EU citizens and is responsible for monitoring a company's approach to data protection making sure that it is in line with the GDPR. The supervisory authority is an independent public authority established by the EU country whose role is to monitor compliance with the GDPR.

But because the GDPR is only a legal framework for resolving a set of very complex technical matters, its implementation is still problematic. Two key aspects of this legislation that are enabling more privacy in the sense of individual control over personal information are the consent withdrawal and the right to be forgotten. However, it is difficult to practically achieve either of these two rights. Namely, practical problems vary from a difficulty to provide a proof that the revocation has been achieved to the impossibility to remove personal data due to the design of mechanisms that protect the privacy of data and many economic and "public-good" reasons which are disabling total consent withdrawal (Politou, et al 2018). But despite the fact that achieving consent withdrawal and the right to be forgotten remains to be a challenge both legally and technologically, the GDPR has revolutionised the way we think about privacy online.

Ever since this legislation has entered into force in May 2018, privacy on the internet has changed its meaning as it is now a shared responsibility. This means that protecting personal data is much less daunting for an individual who has the right to give and withdraw consent thereby gaining more control over his or her own personal data. And even though the GDPR is effectively protecting only EU citizens, it certainly has global implications (Cate et al, 2017; Glinos, 2018; Greengard, 2018). This regulation has raised awareness of privacy protection as a global problem and also led to the transformation of privacy policies in different countries and across different global online platforms. One of these countries is Serbia which, as one of the EU candidate countries, has an obligation to adjust its privacy laws to comply with EU law.

3. ONLINE PRIVACY AND INDIVIDUAL RESPONSIBILITY IN SERBIA

Serbian legislative framework for data privacy is in line with the GDPR to some extent as it introduces the same basic principles such as lawfulness, fairness and transparency, purpose limitation, data minimisation, storage limitation, integrity and confidentiality and accountability[9]. Furthermore, Data Protection Law also lists different actors and divides responsibilities among data subjects, controllers,

[9] Zakon o zaštiti podataka Službeni glasnik RS, 87, 2018, član 5, http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2018/87/13/reg (Accessed: 21.08.2019)

processors and other subjects. However, this legislation has been criticised. According to the 2018 report of the Representative for information of public importance and protection of personal data, the main disadvantages of the Data Protection Law adopted in 2018 are its content that is not in line with the legal system of the Republic of Serbia, provisions that are too broad and there is a long list of limitations which allow many subjects such as governmental bodies and legal subjects access to personal data and disregard the right to privacy which is guaranteed by the Constitution of the Republic of Serbia[10]. Additionally, Representative states that this legislation leaves many problems related to data protection unaddressed or poorly regulated while also stressing out that the text of this law needs significant improvements and that it will inevitably face many challenges when it comes to implementation, especially because the legislation leaves room for various interpretations and is therefore considered as vague.[11]

Due to these drawbacks of the new law and lack of implementation, the responsibility for respecting the right to privacy of citizens of Serbia remains to be an individual responsibility, while other actors fail to recognise their duties in protecting their personal data. Despite the fact that the GDPR has entered into force in May 2018, Serbia has not yet shown its readiness to embrace EU standards for privacy protection and implement regulations that are in line with the GDPS which are included in its data protection laws. Representative for information of public importance and protection of personal data has suggested in one of their official statements that the implementation of the new data protection law should be postponed until 1st of September 2020 and this is due to the fact that this law is a big challenge for public and economic authorities who do not have the capacities to fulfil obligations imposed by this law and also is not capable of investing into projects of raising awareness of the importance of data security or protection of personal data[12]. However, this suggestion has been rejected and the new Data Protection Law has entered into force on 21st of August 2019[13]despite the lack of readiness of the data controllers and processors to start implementing the new law as only 192 of tens of thousands of data controllers have provided data on the person responsible for protection of personal data as it has been stipulated in the Data Protection Law[14].

The fact that there is no readiness and willingness to start implementing the new Data Protection Law which is only partially in line with the GDPR shows that despite the legislation, there is no guarantee that responsibilities for the protection of

[10] Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, Izveštaj o sprovođenju Zakona o pristupu informacijama od javnog značaja i Zakona o zaštiti podataka o ličnosti za 2018. godinu https://www.poverenik.rs (Accessed: 21.08.2019)
[11] Ibid.
[12] Poverenik za informacije od javnog značaja i zaštitu podataka https://www.poverenik.rs/ (Accessed: 21.08.2019.)
[13] Poverenik za informacije od javnog značaja i zaštitu podataka: Početak primene novog Zakona o zaštiti podataka o ličnosti https://www.poverenik.rs/ (Accessed: 22.08.2019)
[14] Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti https://www.poverenik.rs/ (Accessed: 08.09.2019)

personal data will truly be divided among different actors in Serbia. This leaves individuals powerless not only against governmental bodies who are processing personal data for the purpose of national security, crime prevention and other purposes but also against private companies and other subjects who are collecting and processing personal data for economic and other purposes. They are forced to rely solely on their own knowledge and capabilities to protect their personal data.

CONCLUSION

The General Data Protection Regulation has redefined privacy in the age of big data and raised awareness of the problem of personal data protection in the whole world. It has transformed global privacy policies and changed the way many international companies and globally used internet platforms work. Its key innovations are the basic principles which organise the way personal data is being handled with which allow individuals more control over their data. In this sense, a new definition of privacy that emerges does no longer entail the concept of concealment but rather entails the concept of transparency of the process of using personal data. Ultimately, this empowers the individual who is still held responsible and has to give or revoke his or her consent, but the responsibility for their privacy is also shared with other actors such as data controllers, data processors, third parties and other subjects.

Given that the GDPR is onlya piece of legislation which does not provide technical solutions to data privacy, its full implementation is still a big challenge, but it has revolutionised the way privacy is perceived today and gives a solid framework that regulates the right to privacy on the internet. It has its impact globally, however, citizens of countries that are not members of the EU have more responsibility to protect their own data as they are not protected by this legislation. Serbia's new Data Protection Law which has entered into force in August 2019 only partially complies with the GDPR but leaves individuals unprotected especially due to its vague formulations, ambiguities, limitations and lack of implementation. As data controllers and processors are unable to start implementing this law, it seems that there is no real division of duties and individuals are forced to rely on their own capacities to protect their personal data. Understanding the importance of establishing roles and duties of different actors involved in collecting and processing personal data is crucial for Serbia which has to start not just improving their privacy laws to comply with the EU legislation and policies, but also should begin adopting the culture of privacy which is prevalent across the EU states and is mirrored in the GDPR.

BIBLIOGRAPHY

(1) Baker, E. A. (2010) *The New Literacies: Multiple Perspectives on Research and Practice* (ed.). New York and London: The Guildford Press
(2) Baruh, L., Popescu, M. (2015) "Big data analytics and the limits of privacy self-management", *New Media & Society*, Vol. 19, No. 4, 579 – 596

(3) Breakstone, J., McGrew, S., Smith, M., Ortega, T., & Wineburg, S. (2018) "Why we need a new approach to teaching digital literacy". *Phi Delta Kappan*, Volume: 99, Issue: 6, 27–32
(4) Choi, H., Park, J., Jung, Y. (2018) "The Role of Privacy Fatigue in Online Privacy Behaviour", *Computers in Human Behaviour*, Volume 81, 42-51
(5) Gilliom, J., Monahan, T. (2012) *SuperVision: An Introduction to the Surveillance Society*. Chicago: University of Chicago Press
(6) Hajdin M. (2018) "Privacy and Responsibility", in: Cudd A., Navin M. (eds) *Core Concepts and Contemporary Issues in Privacy*. AMINTAPHIL: The Philosophical Foundations of Law and Justice, Volume 8. Springer, Cham
(7) Haggerty, K. D., Ericson, R. V. (2000) "The Surveillant Assemblage", in *British Journal of Sociology* Vol. 51, No. 4, 605-622
(8) Helberger, N., Pierson, J., Poell, T. (2018) "Governing online platforms: From contested to cooperative responsibility", *The Information Society*, Volume 34, Issue 1, 1-14
(9) Heller, C. (2011) *Post-Privacy: Prima leben ohne Privatsphäre*, München: Verlag C. H. Beck Ohg
(10) Friesem, Y. (2019) Teaching Truth, Lies, and Accuracy in the Digital Age: Media Literacy as Project-Based Learning. *Journalism & Mass Communication Educator*, *74*(2), 185–198.
(11) Krish, C. et al (2018) "Bridging the Digital Divide: Measuring Digital Literacy"*Economics: The Open-Access, Open-Assessment E-Journal*, ISSN 1864-6042, Kiel Institute for the World Economy (IfW), Kiel, Volume 12, Issue 23, 1-20
(12) Kuzmanović, D. (2017) *Empirijska provera konstrukta digitalne pismenosti i analiza prediktora postignuća* (doktorska teza). Filozofski fakultet univerziteta u Beogradu
(13) Lyon D. (2010) Surveillance, Power and Everyday Life. In: Kalantzis-Cope P., Gherab-Martín K. (eds) Emerging Digital Spaces in Contemporary Society. Palgrave Macmillan, London
(14) Meyrowitz J. (2002) Post-Privacy America. In: Weiß R., Groebel J. (eds) *Privatheit im öffentlichen Raum*. Schriftenreihe Medienforschung der Landesanstalt für Rundfunk Nordrhein-Westfalen, vol 43. VS Verlag für Sozialwissenschaften, Wiesbaden
(15) Moll, R., Pieschl, S. (2016) "Expecting Collective Privacy: A New Perspective on Trust in Online Communication" in: Blöbaum, B. (Ed.) *Trust and Communication in a Digitized World*, pp 239-251
(16) Moreham, N. A. (2006) "Privacy in Public Places", *The Cambridge Law Journal,* Vol. 65, Issue 03, 606-635
(17) Nissenbaum, H. (1998) "Protecting Privacy in an Information Age: The Problem of Privacy in Public", *Law and Philosophy,* Vol. 17, No. 5/6, 559-596
(18) Pangrazio, L., & Selwyn, N. (2019) 'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data. *New Media & Society*, *21*(2): 419–437.
(19) Politou, E., Alepis, E., Patsakis, C. (2018) "Forgetting Personal Data and Revoking Consent Under the GDPR: Challenges and Proposed Solutions", *Journal of Cybersecurity*, Volume 4, Issue 1
(20) Prlja, S. (2018) "Pravo na zaštitu privatnih podataka u EU", *Strani Pravni Život*, Issue 1, 89-99
(21) Rose, N. (1991) *Governing the Soul: The Shaping of the Private Self*. London: Free Association Books

(22) Rosenthal, S. et al (2019) "A tripartite model of trust in Facebook: acceptance of information personalization, privacy concern, and privacy literacy", *Media Psychology*, DOI: 10.1080/15213269.2019.1648218
(23) Schaar, P. (2009) *Das Ende der Privatsphäre.* München: Wilhelm Goldmann Verlag
(24) Trepte S. et al. (2015) "Do People Know About Privacy and Data Protection Strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS)", in: Gutwirth S., Leenes R., de Hert P. (eds) *Reforming European Data Protection Law*. Law, Governance and Technology Series, volume 20. Springer, Dordrecht
(25) Wrenn, M. V., Waller, W. (2017) "Care and the Neoliberal Individual", *Journal of Economic Issues*, Volume 51, Issue 2, 495-502

SOURCES

(1) General Data Protection Regulation https://gdpr-info.eu/ (Accessed: 08.09.2019)
(2) Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti https://www.poverenik.rs/sr/ (Accessed: 08.09.2019)
(3) Zakon o zaštiti podataka Službeni glasnik RS, 87, 2018, član 5, http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2018/87/13/reg (Accessed: 21.08.2019)

Zbornik IKSI, 3/2019 – I. Stepanović
„Privacy and Digital Literacy: Who is Responsible for the Protection of Personal Data in Serbia?”,
(str. 45-56)

PRIVATNOST I DIGITALNA PISMENOST: KO JE ODGOVORAN ZA ZAŠTITU PRIVATNIH PODATAKA U SRBIJI?

Dok zakoni koji regulišu pravo na privatnost ne uspevaju u potpunosti da zaštite lične podatke zbog kapaciteta za njihovo skladištenje kao i brzine njihovog deljenja i umnožavanja, pojedinci su odgovorni za zaštitu sopstvene privatnosti na internetu. Međutim ovo zahteva specifične tehničke veštine i razvijenu digitalnu pismenost koja podrazumeva stalno obnavljanje znanja o zaštiti privatnosti kao i korišćenje čitavog niza uređaja, softvera, ekstenzijaza internet pretraživače i tehnika za enkripciju. Opšta uredba o zaštiti podataka o ličnosti predstavlja pokušaj da se povrati kontrola nad zaštitom privatnosti te da se odgovornost podeli između različitih aktera, odnosno između korisnika i autoriteta koji kontrolišu ili obrađuju podatke. Ipak, u državama van Evropske Unije čiji građani nisu zaštićeni ovom uredbom, naglasak je mnogo više na individualnoj odgovornosti. Cilj ovo grada je istakne značaj podele odgovornosti za zaštitu privatnosti u Srbiji na različite aktere u društvu.

KLJUČNE REČI: privatnost / lični podaci / digitalna pismenost / digitalni identiteti / Opšta uredba o zaštiti podataka o ličnosti