DOI: https://doi.org/10.56461/ZR_22.DUKPP.10

DIGITAL EVIDENCE AND PROTECTION OF PERSONAL DATA: SOCIOLOGICAL AND LAW ASPECT*

Ana Vuković**

In the era of digitalization, which began in a rudimentary form since the first photograph appeared, the privacy of the individual was transformed from a right to a social privilege. By switching to digitalization of data, instead of memory and written forms, individuals have accepted the change of the right to privacy as one of the basic freedoms in the corpus of human rights. The author points out that in the process of digitalization the change of public / private axis in the use and protection of personal data at the individual level leads to an imaginary sense of universal control through the real consequence of loss of privacy. Sociological and legal aspect of the paper will include an analysis of the process and relationship among digital evidence and protection of personal data. In the conclusion of the paper the author will give an overview of consequences of the use of digital evidence on the right to privacy.

KEYWORDS: *digital evidence, right to privacy, public-private relationship, freedom, control.*

* This paper was written as part of the 2022 Research Program of the Institute of Social Sciences with the support of the Ministry of Education, Science and Technological Development of the Republic of Serbia.

** Ph.D, Research Associate, Institute of Social Sciences, Belgrade, Serbia.

E-mail: *annvukovic@yahoo.com*

1. PROTECTION OF THE RIGHT TO PRIVACY BETWEEN INDIVIDUAL AND SOCIAL: SEPARATION OR MUTUALITY

Violation of the right to privacy is a violation of a person's dignity and in close connection with the evaluation of a human being and understanding of a person as a member of society. The right to privacy is an individual right that should be independent from both the community (in the wider sense society) and the state. However, with the introduction of new technologies, the use of computers, personal mobile phones and the Internet, this right has undergone transformation and disintegration. The transformation is reflected in the fact that it has become part of digital evidence, and by changing the socially desirable pattern of attitudes towards privacy in the context of personal (personal data) protection. Namely, an individual who does not have a collective awareness of the value of each of his personal data, as well as the personal data of another person, may have the opportunity to transform his right and the right to privacy of another person.

Disintegration implies that the right to privacy has suddenly become ubiquitous and everyone's, so that the memory of one act is subject to countless reproductions through everyone's memory in digital form. So, let's say, instead of a few pictures from a social gathering, we have a lot of pictures of everyone present in digital form, which can quickly be spread and become part of the digital archive of other people. Instead of enjoying a moment to remember, the individual separates himself from the mutual vision of the former collective social consciousness and transforms his privacy into a public act, where he exists only if he is present online (Vuković, 2021).

In this way, personal data is multiplied, which can then be found most often on Facebook, Twitter, Instagram and other personal profiles, and, in fact, the common profile of everyone who is on the picture from the previous example. The reason for the accumulation of digital evidence in the form of personal data is depersonalized social relations (internet sociability as a new form of closeness), but the cause can also be narcissism, that is, an individual's obsession with the desire for power through the creation of a parallel social (virtual) reality of an omnipresent self instead of an autonomous personality (Vuković, 2022: 39-41).

In modern conditions, the ideology of family life experienced the abdication of authority and the reshaping of ego. Due to the disintegration of parental authority, there has been a shift from a society in which the dominant values of the superego (values of self-mastery) are in the direction of the glorification of a society in which the values of the id (values of self-indulgence) are recognized. In a milder form, this trend prepares a young person for a way of life in a permissive society oriented to pleasure and consumption (Lasch, 1986: 202).

Speaking about the concept of networked individualism, other authors believe that "the family certainly changes, but it seems that its guardian or rooting role does not change as radically as its structure changes. And other traditional sources of security such as nation, religion or community are also losing their rooting potential much more

slowly than individualization theorists predicted" (Petrović, 2013: 63). "And where traditional institutions lose their importance or disappear carried by the wave of changes in ideas, values or objective conditions of life, new, adapted to the turbulent society, forms of social communication and association arise (*Ibid*. 63)."

Our social capital is represented by the social networks we enter during our lives, in which our private and other social (public) roles are intertwined. In research on whether social capital can be virtual in the sense of whether the Internet plays a key role in the production of social capital, it was observed that "virtual social capital represents one version of network capital", but "it cannot exist without the technology of the Internet, (…) without people, who can (have access) and know (have the necessary skills to use it), as well as without the cyberspace that is created through the Internet (Petrović, 2013: 235).

The basic idea that keeps people in submission (discipline) when it comes to the use of digital forms is the idea that we can no longer live without the Internet and modern technology. According to Foucault, the main means of discipline are space and time, which if used productively form surveillance, where power is invisible, but constantly present (Foucault 1997 according to Antonić, 2021: 236-237). Ways of disciplining when it comes to space are achieved "1. by fencing space (…); 2. by target division of space (…); 3. by functional redistribution of space, i.e. by creating useful space for a specific purpose; 4. by sorting people into appropriate compartments (for example, the class is divided into groups according to success)". Discipline where time is used as a tool involves five moves: "1. dividing time into as clear as possible (and shorter segments); 2. purposeful classification of segments (like a school schedule); 3. linking certain actions to certain segments (dividing actions and placing them in segments); 4. by making different series of actions, arranging them from the simplest to the most complex; 5. By dividing and ranking, that is, by hierarchizing the series of actions, so that each series ends with some threshold)" (*Ibid*. 236).

Does this structuring of time and space for the purpose of disciplining remind you of invisible disciplining in virtual space? Similar principles and rules of new desirable patterns of social behaviour can be observed on the Internet. Every action when sending an email or typing a message on an Android phone, Internet chat rooms as a fence of space for certain social groups and topics, with partitions and subtopics that are discussed virtually, etc.

2. DIGITAL EVIDENCE: INFORMATION ON PERSONALITY

Computers and evidence that can be obtained from the Internet consist of a huge amount of data and information in electronic (digital) form. Our pictures, instant messages, emails, digital transactions, mobile phone clouds, private internet histories, all of these can be used as digital evidence, even though it is private. The common man is often not familiar with the potential ways of archiving digital traces of their activities that may contain personal data and other types of data.

In our legal literature, personal data can be divided based on the degree of confidentiality into "ordinary" personal data and "sensitive" personal data, which are also called "special category" of personal data. The degree of confidentiality is related to the importance that information has for a person. "Ordinary" personal data carry ordinary information about a person, while "sensitive" personal data carry particularly important information about the personal identity of a person. Violation of sensitive personal data, as a rule, produces a more significant consequence for a person than the violation of ordinary personal data. According to this division, sensitive personal data enjoys a higher degree of legal protection than other types of personal data. The group of sensitive personal data includes data on religious and philosophical beliefs, racial and ethnic origin, genetic data, biometric data, data on a person's sexual life and sexual orientation, and data on health status. Other personal data belong to the group of 'ordinary' personal data" (Andonović, Prlja, 2020: 21-2).

In the contemporary world, digitalization represents dehumanization and a form of specific social control, a general surveillance that an individual cannot monitor and control, and cannot be completely absent from (Vuković, 2021: 45). Today, conformism is in the form of "passive acceptance of surveillance technologies" as the price for technical progress, and manifests the weakness of the individual and loss of identity through internalized supervision in consumer society (Subotić, 2011: 265).

Therefore, digital evidence is a link between private and public, it is private to the extent that others cannot access the data, however, with the process of universal digitization of various personal data, this data is at too high risk of becoming public. Therefore, it is debatable whether it is sustainable to divide into less and more sensitive personal data, when they are in digital form. Discussions about the problematic nature of the biometric citizen identification system began in Serbia in 2006, when "the most powerful media houses in Serbia generally affirmed surveillance systems and censored the activities of privacy fighters." (...) For greater control over some population" (Subotić, 2011: 6). The newspaper articles talked about whether and why the chipping of identity cards represents a form of threat to the right to privacy. At the same time, most members of the general population were not informed about what personal data would be on the chip and who would be allowed to read the chip.

Given that the majority of the population of Serbia consists of elderly people who are either not or minimally digitally literate, this meant that they would adapt to the state's decision on the necessity of introducing electronic chipped ID cards. This population is also the one that uses the computer and the Internet less often, but because of this, it is the most vulnerable if it has to do all its obligations, for example paying household bills, exclusively online in the near future.

In the Serbian Criminal Code, Article 146, the unauthorized collection of personal data is regulated: 1) whoever acquires personal data that is collected, processed and used on the basis of the law without authorization, communicates it to another or uses it for a purpose for which it was not intended, will be punished by a fine or imprisonment for up to one year. 2) The penalty from paragraph 1 of this article shall also be imposed

on anyone who collects personal data of citizens against the law or uses such collected data. 3) If the offense referred to in paragraph 1 of this article is committed by an official in the performance of his duties, he shall be punished by imprisonment for up to three years.

Also, the Serbian Criminal Code, among other things, regulates the violation of the right to privacy through violation of privacy of letter and other mail (article 142): "whoever without authorization opens another's letter, telegram or other closed correspondence or consignment or (…) without authorization withholds, destroys or delivers to another person somebody else's letter, telegram or other mail or who violates the privacy of electronic mail will be punished with fine or imprisonment up to two years". And, another article for example, whoever without authorization makes a photographic, film, video or other recording of another thereby significantly violating his personal life or who delivers such recording to a third party or otherwise enables him to familiarize himself with contents thereof, shall be punished with a fine or imprisonment up to one year" (article 144).

The Council of Europe Convention on Cybercrime was signed in Budapest in 2001, to combat the abuse of high technology. Among other things, this convention regulates "group of alleged acts constitutes crimes against computers and computer systems in the strict sense. The Convention has named this group as: Criminal offenses against the confidentiality, integrity and availability of computer data and systems". National Assembly o Republic of Serbia ratified both documents in 2009 and "by ratifying the Convention and Additional Protocol there should essentially have been innovated all laws that directly or indirectly regulated the area of information and communication technologies, and particularly the laws governing criminal-legal protection of these areas" (Zirojević, 2015: 1-2). The European Union's General Data Protection Regulation (GDPR) was adopted in 2016 (replacing the old legal framework from 1995), and implementation began in 2018 (SHARE, 2018).

3. THE POWER OF ONLINE STIGMATIZATION

One of the most well-known definitions of power is the one given by Weber: "power is the prospect of carrying out one's will within a social relationship despite resistance, regardless of what these prospects are based on (Weber, 1976: 37)". In a social relationship, the possession of power, according to Weber, gives us the possibility to impose our own will on the behaviour of others (ibid., 46). This term best describes the individual's desire to impose his will, through the virtual presence of his views and opinions, that is, personal data or data about others.

The shaping of private, and in fact public, opinion on social networks has led to an individual sense of power in the individual. Therefore, the desire for power and wider social recognition, among many people (more or less alienated), has enabled the availability of digital evidence of attitudes and memories. The power in potency and forms

of its possible abuse have complexly marked the floating belonging to the Internet community, and opened wide the door for the private to intertwine with the public, mostly to the detriment of the right to privacy.

Another classic of sociological theory, Parsons defined four forms of influence (persuasion, incentive, obligation activation and coercion), of which only obligation activation represents power, because "power rests on reminding person B that he has undertaken some obligation, that calling (...) to her duties, it is an appeal to her conscience, to the common system of values from which this and that obligation arises" (Antonić, 2021: 133). Internet archives of personal data have the power of potential stigma because they have an unlimited shelf life. Especially when setting up archives about some data that was created in the past.

In the Criminal Code, there is the possibility of deletion from the records after the judgment has expired, the "Internet Code" has its own rules, and data on it, even when they are deleted, for example, can appear on another Internet site. Because personal information is practically any information that can be linked to a specific person. An example of an individual violation of the right to privacy can be a man who was punished a long time ago, and released, but that information remained in the digital archive of an article on the Internet.

An example of the collective threat to the right to privacy in our country is the leaking of information of almost all adult citizens in 2013, when the personal data: first name, last name, middle name, social security number and status of citizens in the records of holders of the right to free shares is more than five million citizens of Serbia who applied for free shares in 2008 and about 4,000 financial documents that were in the database of the Privatization Agency were compromised. In the meantime, the agency was shut down, and the case became statute-barred before the competent authorities (*Ibid.* 2018: 28).

The right to erasure - 'right to be forgotten' is particularly interesting. The exercise of this right can be requested by an individual if "the data is no longer necessary for the purposes for which it was collected, the consent, which was the basis for the processing, has been withdrawn, an objection to the processing has been filed; the data has been processed illegally; the deletion is in accordance with the legal obligation of the operator, the data was collected from the child in connection with the offer of information society services". If the organization has publicly published the subject data, it should inform other organizations that process it, "so that all links to the data or copies are deleted", however, there are also exceptions to this right "when there is an overriding public interest and the organization does not have to act upon request (including freedom of speech, archiving, scientific and statistical purposes, exercise or defence against legal claims)" (SHARE, 2018).

However, experience suggests that an online story can follow some individual years after an event in which they participated took place. The potential abuse of trust in social relations and violation of human dignity even in cases where it is proven that it was not done or that it was falsified remains recorded as an online stigma in the virtual

space. What we can also notice is that the legal regulation, as well as the broader education of individuals in terms of personal data protection and its use as digital evidence, lags behind the amount of personal data that has been left in cyberspace for years. In that sense, "the information society has already shown itself to be a society that brings with it a wide range of unintended side effects, the most important of which can be expressed in terms such as fragmentation, the splitting of time into smaller and smaller parts, and the consequent loss of internal connectivity", in which "the following moment lives parasitically from this moment" (Eriksen, 2003).

CONCLUSION

Considering the changes brought about by digitalization in the modern world, the extension of the definition of the right to privacy has been changed, without the consent of the individual, or more often with unexplained consequences about possible abuses. Although the law cannot legislate all possible legal consequences of the use of personal data, legal regulation has been delayed throughout the world, as it has allowed a few individuals to collect personal data, as well as to set up data archives without the prior consent of the person. Even when there may have been consent, individuals who are digitally illiterate, as well as those who are on average, were not aware of where, when and how they could leave personal data, and especially how they could partially protect it. The social constitution of the numerical abundance of data as an imperative for social progress, instead of organizing complex collective experiences in more direct communication, called into question the connection of generations that were socialized in different social periods, and forced to live in parallel online and offline worlds.

The speed of the flow of personal data and the forms of its circulation leave the potential for the "tyranny of the moment" in one click on the Internet and social networks, and the presence of the personal on the Internet in image and text has become a matter of new social status and prestige that may or may not be rooted in reality. While in classical liberal society the principle was valid: vices are private and virtues are public, in post-capitalist society there is an inversion of public moral principles, so that now there is an insistence on public promotion of human privacy, its control and legal protection. Meandering structures of the personal (private) once existed in the memories of individuals, now they are more often archived on the Internet as a public good.

REFERENCES

1. Andonović, S., Prlja D. (2020) *Osnovi prava zaštite podataka o ličnosti* [*Basics of Personal Data Protection Rights*], Beograd: Institut za uporedno pravo.
2. Antonić, S. (2021) *Moć i poslušnost* [*Power and Obedience*]. Beograd: Srpska književna zadruga.
3. Eriksen, H. T. (2003) *Tiranija trenutka: brzo i sporo vreme u informacionom društvu* [Tyranny of the Moment: Fast and Slow Time in the Information Age], Beograd: Biblioteka XX vek.
4. Krivični zakonik (*Službeni glasnik Republike Srbije*, broj 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019) ["*The Official gazette of RS*"]. Available at: https://www.paragraf.rs/propisi/krivicni-zakonik-2019.html.
5. Lasch, Ch. (1986) *Narcistička kultura* [The Culture of Narcissism]. Zagreb: Naprijed.
6. Petrović, D. (2013) *Društvenost u doba interneta* [*Sociability in the age of the* Internet]. Novi Sad: Akademska knjiga.
7. SHARE (2018) *Vodič kroz GDPR i zaštitu podataka o ličnosti - moji podaci, moja pra*va [*Guide to GDPR and personal data protection - my data, my rights*] Share Fondacija. Available at: https://www.sharefoundation.info/wp-content/uploads/Podaci-u-doba-interneta-Final.pdf.
8. Subotić, O. (2011) *Informaciono kontrolisano društvo* [*Informationally Controlled Society*]. Beograd: Bernar.
9. Veber, M. (1976) *Privreda i društvo* [*Economy and Society*]. Beograd: Prosveta.
10. Vuković, A. (2021) "Responsibility in the Protection of Personal Data and Prevention of Abuse and Crime". In: *Institutions and Prevention of Financial Crime*, (Kostić, J., Stevanović, A., Matić Bošković, M. (eds.)). Beograd: Institut za uporedno pravo, Institut za kriminološka i sociološka istraživanja, 39-48.
11. Vuković, A. (2022) "Kriza uloge porodice i obrazovanja i nasilno ponašanje dece" ["Crisis of the Role of Family and Education and Children's Violent Behaviour"]. In: *Violence and Children*, Zirojević, M. (ed.). Beograd: Institut za uporedno pravo.
12. Zirojević, M. (2015) "Computer related Crime – the Decision of the Council of Europe", *PRAVO – teorija i praksa*, bro*j* 4–6*,* 1-15.

DIGITALNI DOKAZ I ZAŠTITA LIČNIH PODATAKA: SOCIOLOŠKOPRAVNI ASPEKT

U eri digitalizacije, koja je u rudimentarnom obliku počela još od kada se pojavila prva fotografija, privatnost pojedinca se transformisala iz prava u društvenu privilegiju. Prelaskom na digitalizaciju podataka, umesto sećanja i pisanih formi, pojedinci su prihvatili i promenu prava na privatnost kao jednu od osnovnih sloboda u korpusu ljudskih prava. U radu autor ukazuje da u procesu digitalizacije promena ose javno/privatno u korišćenju i zaštiti ličnih podataka na nivou pojedinca dovodi do imaginarnog osećaja sveopšte kontrole kroz realnu posledicu gubitka privatnosti. Sociološkopravni aspekt rada obuhvata analizu procesa i odnosa digitalnog dokazivanja i zaštite ličnih podataka. U zaključku rada autor daje osvrt na posledice upotrebe digitalnih dokaza na pravo na privatnost.

KLJUČNE REČI: *digitalni dokaz, pravo na privatnost, odnos javno i privatno, sloboda, kontrola.*