International Legal Aspects of Mass Surveillance and Implications on Privacy

Siniša S. Domazet and Slavica S. Dinić

Educons University, Faculty of Security Studies, Sremska Kamenica

Article Information*

Review Article • UDC: 343.123.12:342.7
Volume: 19 Issue: 1, page(s): 79–97

Received: February 8, 2022 • Revised: February 27, 2022

Accepted: March 11, 2022

https://doi.org/10.51738/Kpolisa2022.19.1r.5dd

Author Note

Siniša S. Domazet https://orcid.org/0000-0002-5964-2249

Slavica S. Dinić https://orcid.org/0000-0002-7775-8472

We have no known conflict of interest to disclose.

Correspondence concerning this article should be addressed to Siniša s. Domazet, Educons University, Vojvode Putnika 87, 21208 Sremska Kamenica, Serbia.

Email: sdomazetns@gmail.com

* Cite (APA):
Domazet, S. S., & Dinić, S. S. (2022). International Legal Aspects of Mass Surveillance and Implications on Privacy. *Kultura polisa*, *19*(1), 79–97. https://doi.org/10.51738/Kpolisa2022.19.1r.5dd

Kultura polisa
19(1), 79–97

Abstract

The development of modern information and communication technologies, in addition to numerous positive aspects, has also brought challenges to human rights, especially the right to privacy. The paper analyzes the relationship between the practice of mass surveillance and the right to privacy. The acute problem of abuse during the practice of mass surveillance at the international level was pointed out. An analysis of the existing legal framework at the international level was performed, as well as the practice of European institutions. Research has shown that international law does not support modern policies and practices of mass surveillance, which are especially used by the great powers. It has been established that states, especially great powers, resort to the argument that national security is endangered or that there is a danger of terrorism, to justify the practice of mass surveillance. Given the lack of universal legal regulations that would protect the right to privacy from abuse based on the practice of mass surveillance, the solution lies in concluding bilateral agreements or adopting non-binding legal norms. The normative method and legal-logical methods of induction and deduction were used in the research.

Keywords: law, cyber security, privacy, mass surveillance

Kultura polisa
19(1), 79–97

International Legal Aspects of Mass Surveillance and Implications on Privacy

The modern world in the 21st century is characterized by the rapid development of modern technologies, and the rapid flow of information, all of which must be accompanied by appropriate legal regulations. This is especially evident in the field of human rights protection, one of the most important of which is the right to privacy. However, the question arises as to how to reconcile the need to preserve the right to privacy with the interest in preserving national security, protection from terrorist attacks, economic interests or other reasons. Numerous scandals related to the practice of mass surveillance announced in the mass media, and especially the scandal around Edward Snowden, have shown all the complexity of this problem.

At the same time, states and their intelligence agencies are reluctant to reduce their competencies in any way when it comes to national security, which is often not without grounds. Not to mention the complex political relations between East and West on the issue of cyber security. Indeed, there are legal and legitimate reasons that in certain circumstances the wall of inviolability of the right to privacy may be torn down, at least temporarily, to preserve higher goals. But there is a dilemma as to how to draw the line between the need to protect the right to privacy and other human rights on the one hand and the need to protect national interests in situations where they are threatened, especially when it comes to external threats.

In this paper, we analysed these dilemmas, focusing first on the right to privacy, and then analysing the system of mass surveillance and relevant legal regulations at the international level.

The Notion of the Right to Privacy

The accelerated development of information and communication technologies has brought many positive effects on the population and the economy, but at the same time, it has enabled the creation of a system for mass monitoring, surveillance and eavesdropping on communications. With

the development of communication networks, the concept of "networked society" appears as a virtual world in which everyone communicates with everyone. This communication becomes a source of the most diverse information about people. A person is far less careful than in the real world in the virtual world. Apparent invisibility and distance create a feeling of anonymity and security in him, so in certain situations, he gives personal data or undertakes those actions that he would certainly never do in the physical world (Dimitrijević, 2014, pp. 249–250).

The problem of privacy and the right to privacy has long been the result of sharp theoretical debates, with different views expressed. Thus, in the field of intimate relations, the right to privacy was first recognized in a significant case in 1965, Griswold v. Connecticut. In Griswold, the U.S. Supreme Court overturned a Connecticut law banning the sale or use of contraceptives to married couples. The court identified the right to privacy based on the First, Third, Fourth, Fourth and Fifth Amendments to the US Constitution and claimed that the right to privacy in marriage is older than the Charter of Rights (Sarat, 2015, p. 6).

One of the definitions of privacy can also be found in the work of American judges Samuel Warren and Louis Brandais, where the right to privacy is defined as the right to be left alone (Warren & Brandais, 1890, cited in Dimitrijević, 2014, p. 250). In the second half of the twentieth century, this right grew into the right to personal autonomy and consisted of guaranteeing a sphere of personal autonomy within which each individual would have the right to independently, without state interference, regulate their relations with other people. In France, it operates with a unique notion of private life, understood narrowly and with an emphasis on secrecy. In the German doctrine, the right to privacy was very limited until the ruling of the Federal Court in 1954, which recognized the general personal right, and explicitly the right of every person to a secret sphere. The Swiss Civil Code contains a general clause on the protection of the individual which is the legal basis for the protection of the right to privacy. The already determined right to privacy is the absolute subjective right of a natural person to be able to independently decide on the acquaintance of third parties with any manifestation

of his existence. From this right arise especially personal rights such as the right to private life, the right to character, the right to vote, and the right to personal writings (Sinđelić 2012, 9). Kurland defines the right to privacy as a set of three rights: the freedom to intrude on and observe one's private life, the right to maintain control over personal information, and the freedom to act without interference (Kurland, 1976, p. 8).

The problem of privacy has become increasingly important with the development of modern societies and modern technologies and the Internet, and there have been some changes in the definition of this term. Privacy in electronic communications includes the collection, processing and provision of information about the user to third parties, where individuals when recording activities and personal data determine when, how and to what extent information about their private sphere should and can be available to others (Jovanović, 2014, p. 94, cited in: Vilić, 2016, p. 20). Some authors define privacy as a term that encompasses personal autonomy, democratic participation, self-identity management, and social coordination (Cho et al., 2009, pp. 395–416).

According to other authors, the right to privacy does not exist, because any interest protected as a private interest can be equally well protected by some other right, first of all, property or property rights and the right to bodily integrity and security (Jarvis-Thomson, 1975, pp. 295–314). Some authors even claim that the right to privacy, which they want to protect, is economically unprofitable (Posner, 1982, pp. 942–946), and there are views that special emphasis on the need to protect the right to privacy is harmful to women because this right is manipulated, in order for women to be controlled and under the constant domination of men, under the illusion of a desire for their protection (MacKinnon, 1989).

Also, privacy is defined as a political right, but also as a right that exists to protect the interests of citizens (Barnes, 2006). Some authors define the right to privacy as the right of an individual to protection from intrusion into his personal life or business, the life of his family members, either directly by certain actions or by publishing personal information (Shah, 2013, pp. 47–71), or (in the context of social networks) all data that one individual publishes on his profile, which includes pictures, comments,

data on movement and socializing, etc. (King et al., 2011).

Recently, some authors (Boban) are paying more and more attention to the so-called "information privacy", which is a request of individuals, groups or institutions to decide independently when, how and what information about themselves to give to others. According to them, in a broader sense, the concept of information privacy includes information security, which means that an individual in the information society decides when, to whom, how much and how to communicate personal data, taking into account their rights and needs, as well as rights and the needs of the community in which he lives. Information privacy unites the legal values of protection of the rights of individuals in the society of developed information technologies, and this concept of personal data protection, related to communication via electronic networks, is also called "e-privacy" (Boban, 2012, pp. 581–582, p. 595).

After the affair with Edward Snowden, it became clear how important the right to privacy in cyberspace is. This was confirmed by the UN Human Rights Council, as well as the UN General Assembly, which stressed the view that "the same rights that people have offline must also be protected online, including the right to privacy" (United Nations General Assembly, 2015). Privacy is also recognized as a human right in the UN Universal Declaration of Human Rights (Art. 12), as well as in the 1966 International Covenant on Civil and Political Rights.

The most important regional act in Europe, The Convention for the Protection of Human Rights and Fundamental Freedoms, states in Article 8 that "everyone has the right to respect for his private and family life, his home and his correspondence". The Convention stipulates that the suspension of this right may be exercised only when prescribed by law and necessary in a democratic society in the interests of national security, public security or economic well-being, to prevent disorder or crime, to protect health or morals, or to protect the rights and freedoms of others. In addition to this convention, the Council of Europe Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108+), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on

the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and the African Union Convention on Cyber Security and Data Protection should be noted. As regards the national legislation, according to the Report of UNCTAD, 69% of UN Member States have their own legislation regarding the protection of privacy and personal data, 16% of the country does not have regulations in this area, while 10% of the country has made draft appropriate regulations. On the other hand, no data are available for 5% of the countries (UNCTAD, 2020). With regard to the countries that have appropriate laws regarding the right to privacy, it can be said that there is a certain "patchwork". Thus, in some countries, the right to privacy is stated in the constitutions of these countries (i.e., there is a right to privacy is explicitly recognized as a constitutional right).

Second, there are countries where the right to privacy is indirectly regulated by the constitution, as well as regulations in the field of criminal law (examples are the United States). Third, many countries have enacted special regulations governing the protection of personal data, while in some countries the right to privacy is not recognized as an autonomous right (for example, in the United Kingdom and China).

Overall, legal regulations show that countries around the world take the right to privacy very seriously, but the question arises as to how to protect these rights in a world where mass surveillance systems are increasingly present.

Mass surveillance systems

With the development of modern technologies, the lines between the public and private spheres have become blurred, which has led to interference in the right to privacy of incredible proportions. Today, the world is witnessing a significant increase in mass surveillance. After the publication of the data by Edward Snowden in 2013, it became clearer to what extent such supervision goes. Moreover, Snowden's allegations caused a real shock not only to the American intelligence community but also to ordinary citizens around the world, who became aware that their activities

were under constant surveillance. Awareness of constant surveillance of people has forced states and international organizations to deal with the issue of surveillance in two ways, to justify the need for such surveillance, or to advocate the adoption of legal acts that would prohibit this type of surveillance.

At this point, it is necessary to make a distinction between surveillance and mass surveillance, given the scope of these terms. The scope of the notion of surveillance is much broader and according to Bošković it represents "the form and manner of control, supervision, keeping and taking care of something or someone, then the physical or technical activity of protection of objects of security importance, systematic monitoring and control by higher or special bodies for careful observation of one or more business entities (parliamentary oversight or civil oversight), the type of educational measure imposed for the re-education of a juvenile prone to crime, operational police measure of control over professional delinquents, a penitentiary measure of control of convicted persons on the execution of imprisonment and house arrest, operational police measure (secret surveillance)", etc. (Bošković, 2017).

In order to deal further with this issue, it is necessary to define what a system of mass surveillance is. One of the good definitions given by Privacy International is that mass surveillance is the non-selective monitoring of the population or a significant component of a group of individuals (Privacy International, 2020). The practice of mass surveillance is carried out in several ways, which include interception, collection, the transmission of data from e-mail, eavesdropping on telephone conversations, "intrusions" into computers, monitoring and collecting data via social networks, but also collecting so-called metadata (for example, time and place of sending a message or phone call). As for the entities that perform mass surveillance, it would be wrong to think that this is done exclusively by states or entities that work under the direct or indirect control of the state. Moreover, it has been noted that mass supervision can also be performed by private companies, not only on behalf of the government of the member states (on the principle of outsourcing) but also at their own discretion (Leetaru, 2019).

Kultura polisa
19(1), 79–97

It should also be noted that a number of different terms are used in connection with mass surveillance, which has been created by several international organizations and institutions around the world. Thus, the UN General Assembly uses the terms "mass digital surveillance", "online surveillance", and "bulk interception" (Office of the UN High Commissioner for Human Rights, 2014; Emmerson, 2017). The term used by the Venice Commission in its Report on Democratic Oversight of Security Services and the Report on Democratic Oversight of Signal Intelligence Agencies is also interesting, where the term "Strategic surveillance" is used (Venice Commission, 2015). In the case law of the European Court of Human Rights [ECtHR], terms such as "exploratory or generalized surveillance", "bulk interception of communications", or "strategic monitoring" are also used (Klass and Others v. Germany, 1977/1978; Weber and Saravia v. Germany, 2000/2006).

All in all, whatever terminology is used, the practice of mass surveillance and its justification are accompanied by numerous controversies and conflicting views. Proponents of mass surveillance emphasize the need to preserve national security and fight terrorism as the main argument for implementing this practice. They believe that in such cases it is necessary to deviate from the right to privacy and regulations on the protection of personal data for the sake of "higher goals". On the other hand, opponents of mass surveillance point out that this practice should not be allowed at any cost, because it would drastically violate domestic and international human rights guaranteed by domestic and international regulations (right to privacy, freedom of expression, freedom of association, right on personal integrity, the right to health) and violated the basic principles on which modern democracies are based.

The problem with the practice of mass surveillance has especially escalated after the aforementioned affair with Edward Snowden and has initiated numerous debates around the world about the legality and justification of such practices. In this regard, it has been shown that states are often reluctant to enact regulations on foreign non-targeted surveillance of communications, with the European Union noting that almost all Member States have enacted regulations on targeted surveillance, with only a few (France, Germany, the

Netherlands, Sweden and the United Kingdom) also enacted regulations on general (non-targeted) supervision of communications (European Union Agency for Fundamental Right, 2015). Also, it has been shown that countries (especially the most developed ones) rarely want to recognize the use of measures of foreign supervision of communications, given that these activities are most often carried out secretly and often without a legislative basis. The case of Edward Snowden changed that, especially in the United States, where it was admitted that the PRIZMA program was used, and the British government also used that data. This resulted in the passage of the Freedom Act in 2015, which aimed to prevent government agencies from accessing the data of American citizens without a court order. However, the mass surveillance of citizens of other countries remained unregulated. On the other hand, in the UK, under pressure from Snowden's allegations, as well as a special committee of the British Parliament, a special IPA regulation was passed in 2016, one of the most famous regulations on mass surveillance, which actually legalized the procedure of mass surveillance of domestic and foreign communications in Great Britain.

In addition to the above regulations, the activities of international organizations (especially the United Nations) and the non-governmental sector have been noted at the international level, with the aim of protecting the right to privacy in relation to mass surveillance. In this regard, Special Rapporteur Frank La Rue, in his 2013 Monitoring Report, states that "a weak regulatory environment has provided fertile ground for arbitrary and unlawful violations of the right to privacy and freedom of opinion and expression" (United Nations, 2019).

Similar allegations can be seen in the 2019 report of the UN Special Envoy, which points out, among other things, "concerns about technologies that allow the actor to gain covert access to digital communications, intellectual property, data on browsing, research, history location of both online and offline activities of individuals" (United Nations, 2019). The Special Rapporteur, Fionnuala Ní Aoláin, in her Report to the UN General Assembly in 2021, expressed concern about the procurement of new technologies (such as biometric collection technology or passenger name recording infrastructure),

considering the high risk, with wide implications for a range of basic human rights, from the right to life to the right to privacy. It took the position that "capacity building and technical assistance must go hand in hand with the existence or establishment of strong protection of human rights that are institutionally embedded in recipient countries" (United Nations, 2021). The reports of Privacy International do not sound any better (Privacy International, 2018).

The European Court of Human Rights also dealt with mass surveillance in its practice, which, in accordance with the aforementioned Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, examined whether interference by the authorities in the private life of citizens or their correspondence necessary in a democratic society and whether a balance is ensured between the interests of national security, public security or others, ie whether such conduct is in accordance with the law, having in mind the legitimate goals achieved by oversight and whether it is proportionate. In this regard, it is worth mentioning a few characteristic examples.

Thus, in the case of Liberty and Others v. the United Kingdom in 2008, the ECtHR took the view that the action of the British Ministry of Defense against two civilian NGOs from Britain and Ireland, which consisted of intercepting telephone and electronic communications, was contrary to Article 8 of the Convention. A similar position was taken in the case of Roman Zakharov v. Russia in 2016, which referred to the secret interception of mobile telephone communications. Namely, in this case, the Court took the position that the legal regulations in Russia on the mandatory installation of equipment by mobile operators, which enables security agencies to monitor, do not provide sufficient guarantees against abuses related to the interception of communications. The Court also took a negative view in the case of Szabó and Vissy v. Hungary of 2016 with regard to Hungarian legislation on surveillance in cases of suspected terrorism, as well as in the case of Centrum För Rättvisa v. Hungary. Sweden from 2021, also in connection with the interception of communications. In the latter case, the fact that the rules regarding the destruction of intercepted communication

containing personal data, or in the case of cross-border transmission of such data, were not clearly defined. On the other hand, the Court in the case of Kennedy v. The United Kingdom concluded in 2010 that there was no violation of Article 8 of the Convention, given the clearly defined procedures of British law regarding the interception of communications within the country and the lack of evidence in this regard (European Court of Human Rights, 2021).

Conclusion

Based on the above, it can be concluded that international law does not support the modern policy and practice of mass surveillance, which is especially used by the great powers, especially emphasizing the United States and Great Britain. Moreover, there is a growing effort in international law to protect human rights, in this case, the right to privacy, in the best possible way. However, one should be aware of the fact that the development of modern technologies, especially artificial intelligence and the Internet of Things (IoT), will bring with it increasing challenges, so the practice of mass surveillance could be even more harmful than before.

Of course, it cannot be automatically considered that in every situation the practice of mass surveillance is inadmissible, ie that it implies misuse of the collected data. The fact is that in today's world there is a great threat of terrorist attacks, as well as other challenges to national security. It is obvious that countries around the world are resorting to this very argument in order to justify the practice of mass surveillance. It should not be forgotten that international acts (for example, the Convention for the Protection of Human Rights and Fundamental Freedoms) allow derogations from this right when it is prescribed by law and necessary in a democratic society in the interests of national security, public safety or other grounds. Snowden's findings further contributed to efforts to reduce the practice of mass surveillance to the legal framework.

However, with all the efforts to regulate the practice of mass surveillance, it is very difficult to determine the so-called “red line” between the right to privacy as a basic human right and the practice of mass

surveillance. In other words, the key question in the time to come will be when and under what circumstances the right to privacy may be violated in the interest of national security. Taking the side of supporters or critics of the practice of mass surveillance would bring new problems, so it is best to find a "golden mean" between the opposing sides. Finding the answer to this question has long occupied the attention of not only the scientific and professional public but also political elites. At the same time, the attitudes of political elites of different countries are often sharply opposed, which is contributed to the fact that national and regional mechanisms for the protection of the right to privacy are primarily focused on the protection of their territory.

Although there have been several failed initiatives in this area (for example, two drafts of the Code of Conduct on Information Security from 2011 and 2015 by the Shanghai Cooperation Organization, a 2015 proposal from the Council of Europe on intelligence activities, or the 2018 draft UN Legal Instrument on Government and Privacy Oversight), the protection of the right to privacy in relation to mass surveillance is not yet universal. All these attempts to enact universally valid legal acts have met with fierce opposition from many states and their governments, who have pointed out that the proposed documents are unnecessary and that the existing rules of international law provide very good protection of the right to privacy and to protect against abuse in the conduct of mass surveillance practices. When it comes to the Republic of Serbia, the great attention of the scientific and professional public was caused by the draft Law on Internal Affairs from 2021, especially the part that referred to data processing systems. Given the possibility of using automatic technologies, ie parts of video and audio surveillance systems for biometric data processing, to automatically identify persons, and determine time and location, there are great concerns regarding the protection of privacy and personal data and potential abuse.

With all this in mind, the future of mass surveillance is uncertain. Possible legal restrictions of universal nature in order to protect the right to privacy do not seem feasible at the moment, due to excessive differences on this issue, especially between the great powers. A transitional solution

(until the harmonization of universal norms regarding cyber security) would be bilateral agreements, such as the one concluded between China and the United States on cyber economic espionage in 2015, or some kind of non-binding legal norms that would build a basis for mutual trust between states, severely disrupted especially after Snowden's allegations.

References

Barnes, S. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *XI*(9). https://doi.org/10.5210/fm.v11i9.1394

Boban, M. (2012). The right to privacy and the right to access information in the modern information society. Zbornik radova Pravnog fakulteta u Splitu, *XLIX*(3), 581–582.

Cho, H., Rivera-Sanchez, R., & Sun Sun, L. (2009). A Multinational Study on Online Privacy: Global Concern and Local Responses. *New Media & Society*, *XI*(3), 395–416.

Dimitrijević, P. (2014.). *Pravo informacione tehnologije* [Information Technology Law]. Univerzitet u Nišu: Pravni fakultet.

Emmerson, B. (2017). *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism : note / by the Secretariat*. (A/HRC/34/61). United Nations Digital Library. https://digitallibrary.un.org/record/1287357#record-files-collapse-header

European Court of Human Rights [ECtHR]. (2022, January). *Mass surveillance* [Press Unit]. ECHR, Factsheet. https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf

FRA – European Union Agency for Fundamental Rights. (2015). Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Member States' legal frameworks. https://www.statewatch.org/media/documents/news/2015/nov/eu-fra-2015-surveillance-intelligence-services.pdf

Jarvis-Thomson, J. (1975). The Right to Privacy. *Philosophy & Public Affairs*, *IV*(4), 295-314.

Jovanović, S. (2014). Privatnost i zaštita podataka na internetu [Privacy and Data Protection on the Internet]. In V. Urošević (Ed.), *Veze cyber kriminala sa iregularnom migracijom i trgovinom ljudima*. (pp. 87–164).

Ministarstvo unutrašnjih poslova Republike Srbije.

King, J., Lampinen, A., & Smolen, A. (2011). Privacy: Is There An App for That? In L. F. Cranor (Ed.), Symposium on Usable Privacy and Security. (pp. 1–20). SOUPS '11, Pittsburgh, PA, USA – July 20 – 22, 2011. ACM. https://www.jenking.net/files/king_lampinen_smolen_SOUPS_final.pdf

Klass and Others v. Germany (dec.) No. 5029/71, § 51, ECHR 214.

Kurland, P. (1976). The Private. *University of Chicago Magazine*, *69*(1), 8.

Leetaru, K. (2019, June 18). *Much Of Our Government Digital Surveillance Is Outsourced To Private Companies*. Forbes. https://www.forbes.com/sites/ kalevleetaru/2019/06/18/much-of-our-government-digital-surveillance-is-outsourced-to-private-companies/?sh=61cacec31799

MacKinnon, C. (1989). *Toward a Feminist Theory of the State*. Harvard University Press. http://dcac.du.ac.in/documents/E-Resource/2020/Metrial/24Robinson1.pdf

Office of the UN High Commissioner for Human Rights. (2014). *The right to privacy in the digital age*. United Nations. https://digitallibrary.un.org/record/777869

Privacy International. (2018). *Privacy International's response to call for input to a report on the right to privacy in the digital age by the UN High Commissioner for human rights*. OHCR. https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PrivacyInternational.pdf

Posner, R. (1982). The Economic of Justice. *Michigan Law Review*, *LXXX*(4), 942-946.

Privacy International. (2020). Mass Surveillance. https://www.privacyinternational.org/learn/mass-surveillance

Sarat, O. (2015). *A World without Privacy (What Law can and should Do?)*. Cambridge University Press.

Shah, M. (2013). Online Social Networks: Privacy Threats. In R. Chbeir, & B. Al Bouna (Eds.), *Security and privacy preserving in social networks*. (pp. 73-94). Springer.

Sinđelić, Ž. (2012). Pravo na privatnost-krivičnopravni, krivičnoprocesni i kriminalistički aspekti [Right to Privacy-Criminal, criminal, Procedural and Criminalistic Aspects]. (Doctoral dissertation). http://doiserbia.nb.rs/phd/fulltext/BG20120704SINDJELIC.pdf

Surveillance (2017). In M. Bošković, *Leksikon bezbednosti* [Security Lexicon]. Službeni glasnik.

UNCTAD. (2020). Data Protection and Privacy Legislation Worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

United Nations General Assembly. (2015, February 10). The right to privacy in the digital age: resolution. (A/RES/75/176). United Nations Digital Library. https://digitallibrary.un.org/record/3896430?ln=en

Human Rights Committee. (2019, May 30). Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. (A/HRC/41/35/Add.2) (Excerpts). United Nations. https://www.un.org/unispal/document/report-of-the-special-rapporteur-on-the-promotion-and-protection-of-the-right-to-freedom-of-opinion-and-expression-a-hrc-41-35-add-2-excerpts/

United Nations High Commissioner for Human Rights. (2021). Promotion and protection of the human rights and fundamental freedoms of Africans and of people of African descent against excessive use of force and other human rights violations by law enforcement officers. (A/HRC/47/53). United Nations Digital Library. https://digitallibrary.un.org/record/3930167#record-files-collapse-header

Venice Commission. (2015). Update of the 2007 Report on the Democratic Oversight of the Security Services and the Report on the Democratic

Oversight of Signals Intelligence Agencies. Council of Europe. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e

Vilić, V. (2016). Povreda prava na privatnost zloupotrebom društvenih mreža [Violation of Right to Privacy on Social Networks as a Form of Cyber Criminality][Doctoral dissertation, University of Niš: Faculty of Law). http://www.prafak.ni.ac.rs/files/disertacije/dis-vida-vilic.pdf

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220. https://www.jstor.org/stable/1321160?seq=1

Weber and Saravia v. Germany (dec.) No. 54934/00, § 4, ECHR 2006-III.

Kultura polisa
19(1), 79–97

Međunarodnopravni aspekti masovnog nadzora i implikacije na privatnost

Siniša S. Domazet i Slavica S. Dinić

Univerzitet Edukons, Fakultet za studije bezbednosti, Sremska Kamenica

Sažetak

Razvoj savremenih informaciono-komunikacionih tehnologija pored mnogobrojnih pozitivnih strana doneo je i izazove za ljudska prava, a posebno pravo na privatnost. U radu je izvršena analiza odnosa između prakse masovnog nadzora i prava na privatnost. Ukazano je na akutni problem zloupotreba prilikom vršenja prakse masovnog nadzora na međunarodnom planu. Izvršena je analiza postojećeg pravnog okvira na međunarodnom planu, kao i prakse evropskih institucija. Istraživanje je pokazalo da međunarodno pravo ne podržava savremenu politiku i praksu masovnog nadzora kojim se naročito služe velike sile. Utvrđeno je da države, posebno velike sile, pribegavaju argumentu da je ugrožena nacionalna bezbednost ili da postoji opasnost od terorizma, kako bi opravdale praksu masovnog nadzora. S obzirom na nepostojanje univerzalne pravne regulative kojom bi se pravo na privatnost zaštitilo od zloupotreba po osnovu prakse masovnog nadzora, rešenje je u zaključenju bilateralnih sporazuma, ili usvajanju neobavezujućih pravnih normi. U istraživanju su korišćeni normativni metod i pravno-logički metodi indukcije i dedukcije.

Ključne reči: pravo, sajber bezbednost, privatnost, masovni nadzor