UDC: 342.721:004.056
DOI: 10.5937/PDSC25546M

Darko M. Marković, PhD, Associate Professor
Faculty of Law for Commerce and Judiciary in Novi Sad,
Business Academy University in Novi Sad
email: darko.markovic@pravni-fakultet.edu.rs
https://orcid.org/0000-0001-9124-6417

Mina Zirojević, PhD
Senior Research Associate,
The Institute of Comparative Law, Belgrade,
email: mina.zirojevic@gmail.com
https://orcid.org/0000-0001-9884-5615

JUSTICE IN THE DIGITAL SOCIETY: LEGAL FRAMEWORKS FOR ADDRESSING ETHICAL CHALLENGES IN CYBERSECURITY

Abstract:

Digital society is the result of technological progress, but in addition to the numerous advantages it offers, it also represents a major security challenge, primarily in cyberspace. In addition to being a challenge for the digital society itself, cybersecurity faces ethical challenges that accompany efforts to reconcile surveillance with the right to privacy, accountability for cyber incidents, and the protection of critical infrastructure. Addressing these challenges requires comprehensive and clear legal frameworks. This paper explores how legal frameworks can contribute to justice in the context of addressing these challenges, focusing on the ethical and social implications. The goal of the paper is to analyze existing international and national legal solutions to identify their shortcomings and, according to their characteristics, propose improvements that would enable better protection for individuals and societies in the digital environment. To achieve this goal, including the evaluation of the effectiveness of legal responses, a methodological framework was applied that combines a theoretical and practical approach, which is based on a qualitative analysis of the most important legal documents and existing references on ethics and cybersecurity policy, as well as practical analyses of real examples of cyber incidents. The expected outcome is recommendations for the development of legal frameworks based on equity – establishing a balance between security needs and ethical principles. Such a balance would improve citizens' trust in digital systems and, at the same time, strengthen the security of the digital society.

Keywords: *privacy, liability, law, security challenge, critical infrastructure*

1. INTRODUCTION

The digital space is no longer just a technological innovation – it has become an indispensable segment of modern society, where key processes of communication, business

and information management take place. However, its development does not always follow a proportional adaptation of legal and ethical norms, leading to growing challenges in the field of privacy, surveillance and legal liability for cyber incidents. This paper investigates precisely these legal and ethical dilemmas, analyzing how different regulatory approaches are reflected at the global, European and national levels.

The methodological procedure includes the analysis of legal sources, international norms and sectoral regulations, while considering concrete examples from practice that point to the limitations of existing legal solutions. The primary goal of the research is to determine the key challenges in the regulation of cybersecurity and the identification of legal mechanisms that can contribute to strengthening the protection of data and infrastructure.

Research results confirm that the legal system fails to keep pace with technological development, while political and social differences make it difficult to harmonize regulations internationally. The analysis shows that GDPR[1] and NIS2[2] are effective models of data protection and cybersecurity in the EU, but their application outside the Union depends on the institutional capacities of individual states. The research indicates that Serbia, despite striving towards European integration, not only has to adapt its laws, but also improve their practical application. The observed problems, such as mild punitive measures and slow administrative reactions, point to the need to strengthen legal mechanisms, transparent data management and investments in digital infrastructure, in order to ensure effective cybersecurity.

2. CYBERSECURITY AND ETHICAL CHALLENGES

Cyber security is a necessary response for users of the digital space to numerous dangers, embodied to the greatest extent through data theft, system hacking and manipulation of information flows. Establishing a system of preventive and reactive measures against cyber threats has grown into a functional imperative of digital society.[3] The challenges in the construction and functioning of such a system are not only of a technical but also of a legal nature, considering that it is necessary to establish a balance between the protection of the individual and the need for surveillance, as well as to assume responsibility for cyber incidents and the protection of critical infrastructure. For a deeper investigation of legal frameworks in further work, it is necessary to first consider the challenges related to privacy, responsibility and infrastructure protection. In the following, we analyze the key ethical dilemmas that always arise when talking about cybersecurity, and through this short analysis we indicate the legal framework for considering these challenges. In the analysis, we rely on international and national regulations, as well as real practices, including ethical considerations, in an effort to highlight the need for just solutions that can reconcile security needs with the principles of justice and fairness.

1 European Parliament and Council. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. (2025, May 30) Retrieved from: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

2 European Parliament and Council. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union*. (2025, May 29) Retrieved from: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

3 Zirojević, M., & Ivanović, Z. (2022). *Cyber Law – Serbia*. Belgrade: Institute of Comparative Law.

2.1. Privacy and Surveillance in Digital Space

Digital society implies the inclusion of numerous digital technologies in the daily activities of citizens. Citizens themselves individually, and especially state institutions and organizations, as well as numerous business entities, undertake various security measures in order to counter numerous cyber threats in a timely manner. From the point of view of security, these measures are completely justified and necessary, but they are often not in balance with citizens' right to privacy. This especially applies to the increasingly common practice of mass surveillance, not only by state elements, which is why the question is often raised where the limits of ethical and legal justification of such activities are.

Privacy and Surveillance Legal Framework

Although data protection laws have developed significantly in recent times, ethical issues, including liability issues, are still present, which in some ways is not easy to avoid given the dynamic development of digital technologies. While in the US these laws are fragmented with large powers of government authorities to access private data,[4] the General Data Protection Regulation (GDPR) in Europe sets standards that everyone must adhere to in order to preserve the protection of citizens' data.[5] For example, Meta was fined 405 million euros in 2022 for breaching the GDPR, which points to strict European standards.[6]

Conflict: privacy or security?

Given the variety and sophistication of security challenges in the digital environment, which are practically impossible to avoid, surveillance methods that include monitoring of mass communications and biometric identification seem truly justified. However, these methods are not harmless, because they are applied by humans, which automatically includes the risk of abuse. The PRISM program, revealed in 2013, shows how mass surveillance by government agencies violates citizens' privacy, prompting ethical and legal criticism.[7] Transparency and accountability are the main issues, the answers to which are expected to enable the creation of unambiguous legal rules that regulate surveillance without jeopardizing the basic rights and freedoms of citizens.

A Comparative Overview of Global Strategies

While in the EU privacy rights are more tightly controlled, in the US there is a national security approach, where government agencies have the power to collect data to stop cyber threats.[8] China and Russia have extensive digital surveillance policies, whose legal systems greatly restrict personal rights. Thus, China's 2017 Cyber Security Law

4 For example: California Legislature. (2020). *California Consumer Privacy Act, Cal. Civ. Code § 1798.100.* (2025, May 29) Retrieved from: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5&part=4.&chapter=&article=

5 European Parliament and Council. (2016). *Regulation (EU) 2016/679*, *op. cit*.

6 Data Protection Commission. (2022). *Data Protection Commission announces decision in Instagram Inquiry*. (2025, May 30) Retrieved from: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-instagram-inquiry

7 Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. New York: Metropolitan Books, p. 92.

8 U.S. Congress. (2001). *USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272.* (2025, May 29) Retrieved from: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf

requires data localization, limiting privacy in favor of state control.[9] Ultimately, with well-defined systems of control, accountability, and openness in the enforcement of surveillance programs, the legislative response to these issues should ensure a balance between cybersecurity and privacy protection.

2.2. Liability for Cyber Incidents

Given that digital infrastructure is at the core of modern society, increasingly frequent cyber incidents require us to re-examine who and how bears responsibility – legal as well as ethical. Since cyber space is characterized by anonymity and cross-border, the process of determining responsibility is further complicated. Individuals, organizations and countries face numerous challenges in trying to find an effective mechanism to respond to such threats. Therefore, it is crucial to establish a balance between valid legal norms and ethical principles, in order to ensure adequate protection of victims and preserve justice in the digital environment.[10]

Legal Framework of Liability

Legal systems largely recognize cybercrime as a serious threat, defining forms of liability through various legal mechanisms. However, their application often remains limited by the complexity of cyberspace – especially when it comes to attacks involving multiple jurisdictions or actors with political protections. The Budapest Convention on Cybercrime (2001) encourages international cooperation and harmonization of legal solutions, but its effectiveness is questioned when incidents involve state entities.[11] At the national level, an example is the Law on Information Security of the Republic of Serbia (2016), which, among other things, stipulates the obligation to report on security incidents.[12] However, in practice, mechanisms for rapid response and cross-border cooperation remain underdeveloped, which significantly reduces its applicability in complex cases.[13] A good indicator of these shortcomings is the case of the attack on Equifax (2017), in which more than 147 million user accounts were compromised. Although the company was fined $575 million, the extent of justice for affected users remains disputed.[14]

9 Standing Committee of the National People's Congress. (2017). *Cybersecurity Law of the People's Republic of China*. (2025, May 30) Retrieved from: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

10 Marković, D. M., & Zirojević, M. (2024). Izazovi u regulisanju i identifikaciji *deepfake* sadržaja [Challenges in regulating and identifying deepfake content]. U M. Počuča (Ur.), *Odgovori pravne nauke na izazove savremenog društva – zbornik radova sa naučnog skupa*. (str. 679–692). Novi Sad: Univerzitet Privredna akademija. DOI: 10.5937/PDSC24679M.

11 Council of Europe. (2001). *Convention on Cybercrime (ETS No. 185).* (2025, May 29) Retrieved from: https://www.coe.int/en/web/cybercrime/the-budapest-convention

12 Zakon o informacionoj bezbednosti [Law on Information Security], *Službeni glasnik RS*, br. 6/2016, 94/2017 i 77/2019, Art. 15.

13 European Commission**.** (2023). *Serbia 2023 Report (SWD(2023) 695 final).* (2025, June 1) Retrieved from: https://enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_695_Serbia.pdf

14 Federal Trade Commission. (2024). Equifax Data Breach Settlement. (2025, June 2) Retrieved from: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

Ethical Dimension

Responsibility in cyberspace cannot be viewed exclusively through a legal lens. The ethical perspective introduces additional requirements that are not only limited to punishing perpetrators, but also include proactive prevention of harm, as well as respect for the fundamental values of digital justice. In a world where cyber-attacks are becoming more sophisticated and the lines of liability increasingly blurred, ethics are becoming crucial to fill the gaps that the law still fails to cover.[15]

One striking example is the 2017 NotPetya attack, which led to billions of dollars in economic damage worldwide, including the financial, logistics and healthcare sectors. Although actors connected to state structures are responsible for the attack, legal responsibility has never been formally established, mostly due to complex geopolitical relations and the absence of universal mechanisms for sanctioning states in cyberspace.[16]

The Way to Just Solutions

Such cases show that ethical responsibility must go beyond the boundaries of the law. Organizations that manage large amounts of user data should adopt approaches based on the principle of "social responsibility", even when formal rules do not require it. Also, states should establish rules of behavior in cyberspace that will be in line with international norms, with mutual respect for digital sovereignty.[17] Otherwise, we risk that cybersecurity remains an unregulated field where the interests of power are placed above the interests of justice.[18]

2.3. Protection of Critical Infrastructure

Critical infrastructure – such as energy grids, financial systems, healthcare and transportation – is becoming increasingly reliant on digital technologies, making it particularly vulnerable to cyber threats. Cyber security in this domain goes beyond technical issues and penetrates into the area of protection of basic social functions, thus acquiring both legal and ethical dimensions.

In many countries, the protection of these systems is recognized as a strategic priority, but approaches vary. The European Union established the NIS Directive (2016), which obliges operators of key services to meet security standards and report incidents.[19] In Serbia, a similar principle was introduced through the Law on Information Security, but its implementation still depends on the capacity of individual sectors and technical maturity.[20]

On the other hand, numerous cyberattacks on infrastructure – such as the incident in the Ukrainian power system (2015) or the attack on the Colonial Pipeline in

15 Marković, D. M., & Zirojević, M., *op. cit.*

16 Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York: Doubleday, p. 204.

17 Council of Europe, *op. cit.*

18 Marković, D. M., & Zirojević, M., *op.cit.*

19 European Parliament and Council. (2016). *Directive (EU) 2016/1148 on measures for a high common level of security of network and information systems across the Union.* (2025, June 1) Retrieved from: https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng

20 Zakon o informacionoj bezbednosti, *op. cit*.

the USA (2021) – show that legal regulation often comes after the fact, as a reaction to the consequences.[21] In such an environment, the ethical aspect plays a key role: organizations would have to act not only in accordance with the law, but also in the spirit of social responsibility, especially when it comes to the safety of citizens.

That is why it is necessary to develop models of cooperation between the state, the private sector and civil society, which will enable not only adequate protection of the infrastructure, but also transparency, trust and resilience of the system as a whole.

3. LEGAL FRAMEWORK AND REGULATIONS

The digital society faces challenges that go beyond the purely technical aspects of cybersecurity, requiring clear legal frameworks that can balance the protection of individuals with broader security interests. As shown in previous analyses, privacy, accountability and protection of critical infrastructure represent key dimensions of these challenges, but without legal support, ethical dilemmas remain unresolved.

An effective response to cyber threats requires a balance between security measures and citizens' rights, but legal systems often lag behind in adapting to these challenges, especially due to the complex nature of the digital space. This section discusses international and national regulations, with special reference to the position of Serbia in relation to European legal standards. Through the analysis of key norms, a comparative review of legislative solutions and the identification of legal gaps, we will point out the possibilities of improving legal protection in the digital environment.

Legal regulation in cyberspace is expected to balance security and respect for the basic rights of citizens. If the norms were not clear and applicable, ethical principles would be just a dead letter on paper. This analysis seeks to point out concrete legal steps that can contribute to shaping a safer digital society, in which justice is administered through laws adapted to cybersecurity challenges.

3.1. International legal standards

International legal regulation lays the foundation for cybersecurity, but often faces the challenge of adapting to accelerated technological progress. The European GDPR from 2018 brings strict data protection norms, obliging organizations to transparent and responsible handling of users' personal information. The €405 million fine against Meta in 2022 for privacy violations shows the power of the GDPR, but also the complexity of its global application.[22]

On the other hand, the Budapest Convention[23] seeks to improve international cooperation in the fight against cybercrime, including the protection of critical

21 Easterly, J., & Fanning, T. (2023, May 7). *The attack on Colonial Pipeline: What we've learned & What we've done over the past two years.* Cybersecurity and Infrastructure Security Agency (CISA). (2025, June 2) Retrieved from: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

22 Data Protection Commission, *op. cit*.

23 Council of Europe*, op. cit*.

infrastructure, but it also has its shortcomings, which is not surprising considering that a lot has changed in the digital world for a quarter of a century of its existence. Even without those changes, it can be objected to this convention that it does not fully cover ethical dilemmas, such as mass surveillance, which still remains legally problematic. The NIS2 Directive (2022) is a modernized legal regulator of activities in cyberspace and, accordingly, requires EU member states to undertake the necessary activities in order to each improve cybersecurity in the most important sectors, the most important of which are health and energy industry.[24] However, it is precisely in that implementation that the problem arises, because the member states have their own challenges in adapting these norms to their legal system.

In practice, there are numerous examples that show that legal frameworks do not always succeed in establishing a balance between security and ethical norms. Snowden revealed to us that the PRISM program (2013) encroached on people's privacy, both in breadth and in depth - thus, not taking into account the right to privacy in the slightest. [25] If we compare the compliance of legal and ethical standards in other similar societies – the EU and the USA – we also see a discrepancy that makes it difficult to harmonize global standards, because while the GDPR protects citizens' data, the American Patriot Act (2001) enables broad surveillance, often without judicial approval.[26] In another part of the world, in China, which is a globally extremely important political factor in the international order, the challenge is the Cyber Security Law (2017), which mandates the localization of data and limits the digital rights of users.[27]

These examples show how the inconsistency of safety with ethical norms manifests itself in practice, that is, in real situations. The creation of legal regulations is not simple, but requires a very good understanding of the characteristics of cyberspace in order to simultaneously protect citizens from abuses and ensure a balance between security and freedom. It is clear that in order to fulfill that goal – better regulation of cyberspace – it is necessary to improve international cooperation, and it could start with the reform of the Budapest Convention, which requires political will and clear ethical standards.

3.2. Legal Frameworks of Cybersecurity: Challenges and Improvement in Serbia and Globally

Serbia is a candidate for EU membership, and this imposes numerous obligations on it to comply with EU legislation, and the slowness of this process shows that there are numerous challenges for Serbia on that path. When drafting the Law on the Protection of Personal Data,[28] care was taken to be compliant with the GDPR – not in the sense of rewriting all GDPR provisions, but in terms of emphasizing the necessity of achieving transparency

24 European Parliament and Council. (2022), *op. cit*.

25 Greenwald, G. *op. cit*.

26 American Civil Liberties Union. (2001). *Surveillance under the USA/PATRIOT Act.* (2025, May 29) Retrieved from: https://www.aclu.org/documents/surveillance-under-usapatriot-act

27 Stanford DigiChina. (2017). *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017).* (2025, May 29) Retrieved from: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

28 Zakon o zaštiti podataka o ličnosti [Law on the Protection of Personal Data], *Sl. glasnik RS,* br. 87/2018.

and consent for data processing, including the "right to be forgotten".[29] The effectiveness of the law is always demonstrated by its applicability in practice and, accordingly, by the influence on the behavior of those to whom the provisions are applied. Thus, in this case, it can be remarked that this Serbian law does not have a strong deterrent effect like the GDPR, not only because it does not match the GDPR completely, but also because of much lighter penalties than in the EU - while the GDPR allows fines of up to 20 million euros, the Serbian law foresees much lower amounts. When it comes to the Law on Information Security, there are also problems with its effectiveness, but these problems are of a different nature – the lack of resources and expertise for risk management, which hinders operators of critical infrastructures in fulfilling the obligations imposed by this law.[30] This is especially evident in sectors such as healthcare, where cyber attacks are becoming more frequent.

The problem that Serbia has not solved is the development of mechanisms for quick response, which the NIS2 Directive ordered as a strict obligation for EU member states, where both obligations are especially emphasized for the most sensitive strategic sectors, such as health and energy industry. The importance of readiness to provide an effective legal response to cyber threats was demonstrated in 2021 by the example of attacks on Irish hospitals.[31] Serbia has not recorded such incidents, but that does not mean that they cannot happen in the future. On the contrary, insufficient readiness to respond is a vulnerability that itself attracts a potential attack. Jurisdiction is an additional challenge, as cyber threats cross borders and the Budapest Convention does not always ensure cooperation, as in the case of the 2017 NotPetya attack, where responsibility was not established.[32] Attribution is also a problem, as anonymity makes it difficult to identify perpetrators, leaving victims without justice. In order for Serbia to be able to meet such high standards of the EU, it would have to improve its ability to coordinate, but also allocate significant financial resources for these needs.

There are also different challenges in other parts of the world, which arise from their specificities, which is why there are different legal approaches in relation to the EU. For example, the USA does not have a single, comprehensive law on the federal level like the GDPR in the EU, which is why legal fragmentation occurs in this area – individual American states pass their own laws, which often differ from the laws of other states, and even from federal regulations.[33] China, on the other hand, as we have already stated, uses the Cyber Security Law (2017) to strictly control data and citizens. But these are other parts of the world, other continents and different positions of those countries in the international order – far stronger than Serbia has. In order to improve, Serbia needs to increase penalties and allocate resources, and globally, stronger cooperation and ethical principles, such as transparency, are needed to prevent abuses such as mass surveillance or deepfakes.

29 The right to require internet search engine operators to remove links to certain content on all domains used by the search engine. See: Mladenov, M., & Stojšić Dabetić, J. (2021). Ažuriranje „prava da se bude zaboravljen" kao principa zaštite podataka u Evropskoj uniji [An update on the right to be forgotten as a principle of personal data protection in European union]. *Kultura polisa*, *18*(44), 99–109, DOI: 10.51738/Kpolisa2021.18.lr.2.04.

30 Zakon o informacionoj bezbednosti, *op. cit*.

31 Tidy, J. (2021, May 21). *Irish cyber-attack: Hackers bail out Irish health service for free.* BBC News. (2025, June 2) Retrieved from: https://www.bbc.com/news/world-europe-57197688

32 Schmitt, M., & Biller, J. (2017). *The NotPetya cyber operation as a case study of international law.* EJIL: Talk! (2025, June 2) Retrieved from: https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/

33 DLA Piper. (2024). *Data protection laws in the United States.* (2025, June 2) Retrieved from: https://www.dlapiperdataprotection.com/index.html?t=law&c=US

Although the legal framework for the protection of personal data in Serbia exists, its implementation remains full of challenges. Criminal law data protection is insufficiently developed, and prosecution offices rarely process reports of violations, which leaves citizens without adequate protection.[34] In the health and education sectors, transparency of data management is problematic, particularly through systems such as the COVID-19 IS and JISP. A special risk is brought by mass video surveillance, the regulation of which is not adapted to the technological standards of privacy protection.[35] On the other hand, the new Law on Social Cards introduces broad data collection, but without clear guarantees of user protection. Unregulated international data transfers further complicate the situation, especially after the cancellation of the Privacy Shield mechanism for data transfers to the US.[36] This repeal occurred in July 2020 because the European Court of Justice found that the Privacy Shield does not provide sufficient protection against American surveillance of the data of European citizens.[37] In order to ensure a satisfactory level of data security, it was necessary to switch to alternative mechanisms, such as standard contractual clauses or special agreements between companies,[38] until 2023, when the European Commission adopted a new framework – the EU-US Data Privacy Framework.[39] Serbia is not a member of the EU and is not directly subject to the decisions of the European Commission, so it is not part of that legal framework, so according to the decision of the Government of Serbia, the free transfer of data to the USA is allowed, as a country with an "adequate level of protection".[40] If it wants to be recognized as a country that adopts the highest standards in the field of cybersecurity, those required by the legal framework of the EU, Serbia must improve its regulations with European standards, not only in terms of protection but also in terms of penalties and resources. Justice in a digital society requires that citizens be protected from cyber threats, and from the point of view of citizens' right to privacy and excessive surveillance, it is a kind of cyber threat, and this problem must also be brought into the appropriate legal and ethical framework. Alignment with the GDPR and NIS2 is an obligation that Serbia itself has accepted, and certainly it can help, but in order for the alignment to be not only formal, but also practical in terms of effective application of the law, public education is also necessary.

34 Marković, D. M., & Marković, D. (2025). Cybercrime and law – managing challenges and prospects in the digital age. *Pravo – teorija i praksa*, *42*(2), 49–61. https://doi.org/10.5937/ptp2502049M

35 Domazet, S., Marković, D. M., & Skakavac, T. (2024). Privacy under threat – The intersection of IoT and mass surveilance. *Pravo – teorija i praksa*, *41*(3), 109–124. DOI: 10.5937/ptp2403109D.

36 Partners Serbia. (2021). *Privacy and personal data protection in Serbia: An analysis of selected sectoral regulations and their implementation.* Partners for Democratic Change Serbia. (2025, June 2) Retrieved from: https://partners-serbia.org/public/documents/Privacy_and_Personal_Data_Protection_in_Serbia-_An_Analysis_of_Selected_Sectoral_Regulations_and_Their_Implementation,_PS.pdf

37 European Commission. (2023). *EU-US data transfers.* European Commission. (2025, June 2) Retrieved from: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en

38 Schoenherr. (2023). *Rethinking EU-US personal data transfers and their effect on transfers from Serbia.* Schoenherr. (2025, June 2) Retrieved from: https://www.schoenherr.eu/content/rethinking-eu-us-personal-data-transfers-and-their-effect-on-transfers-from-serbia/

39 McGinnis, B. J., & Blaney, M. S. (2023). *European Commission adopts adequacy decision for EU-U.S. Data Privacy Framework.* National Law Review. (2025, June 2) Retrieved from: https://natlawreview.com/article/european-commission-adopts-adequacy-decision-eu-us-data-privacy-framework

40 Schoenherr, *op. cit*.

4. CONCLUSION

Cyberspace is a modern reality, which attracts the attention of outsiders not only as a technological phenomenon, but also as a legal and ethical challenge. The issue of privacy, surveillance and responsibility for cyber incidents is considered in many legal systems, and practice has already shown that the establishment of international standards is a prerequisite for obtaining quality answers to these questions. With regulations like GDPR and NIS2, the EU seems to have set very successful standards that help not only EU members but also countries that aspire to EU integration, such as Serbia, to try to answer not all the challenges brought by activities in cyberspace.

Globally, the diversity of legal approaches represents a difficulty on the way to establishing universal international standards, and the nebulousness of cyberspace borders can be effectively overcome only by harmonizing legal standards at the international level. This seems to be an impossible undertaking for now, because the creation of legal approaches is conditioned by social and political differences, which are mostly reflected through the prism of the main players on the international political scene – the EU insists on privacy, the USA supports broad surveillance with its Patriot Act, and China legalizes the control of digital space. In order to overcome such differences and establish uniform standards, reforms such as the modernization of the Budapest Convention are necessary.

Not only because it strives for European integration, Serbia must improve its approaches to data protection and cybersecurity, because there are numerous problems that need to be overcome – from mild punitive measures to slow adaptation to new requirements. Serbia must make an effort to harmonize its regulations in this area with European norms, and more than that – to improve the practical application of the legislation. In order to achieve this, it is necessary to strengthen resources and capacities for a faster response to cyber threats, increase transparency in data management, and all of this requires greater investments in the digital space. These investments do not only mean financial resources, although everything else depends on them – to build a sustainable cybersecurity system, it is necessary to invest in the education of citizens and the development of ethical responsibility of institutions. With the achievement of these goals, conditions will be created for the achievement of the main goal - effective cybersecurity built on a compromise between the needs to protect the technological infrastructure and the basic rights of individuals.

Dr Darko M. Marković, vanredni profesor
Pravni fakultet za privredu i pravosuđe u Novom Sadu,
Univerzitet Privredna akademija u Novom Sadu
email: darko.markovic@fepps.edu.rs

Dr Mina Zirojević, viši naučni saradnik
Institut za uporedno pravo, Beograd,
email: mina.zirojevic@gmail.com

PRAVDA U DIGITALNOM DRUŠTVU: PRAVNI OKVIRI ZA ADRESIRANJE ETIČKIH IZAZOVA U SAJBER BEZBEDNOSTI

Apstrakt:

Digitalno društvo je rezultat tehnološkog progresa, ali pored brojnih prednosti koje nudi predstavlja i veliki bezbednosni izazov, pre svega u kibernetskom prostoru. Pored toga što i sama predstavlja izazov za digitalno društvo, sajber bezbednost se suočava sa etičkim izazovima koji prate napore za usklađivanje nadzora s pravom na privatnost, odgovornost za kibernetske incidente i zašitu kritične infrastrukture. Rešavanje ovih izazova zahteva sveoubhvatne i jasne pravne okvire. Ovaj rad istražuje na koji način pravni okviri mogu doprineti pravdi u kontekstu rešavanja ovih izazova, pri čemu težiste stavlja na etičke i društvene implikacije. Cilj rada je da se analizom postojećih međunarodnih i nacionalnih pravnih rešenja uoče njihovi nedostaci i, shodno njihovim obeležjima, predlože poboljšanja koja bi omogućila bolju zaštitu pojedinaca i drutšva u digitalnom okruženju. Za ostvarenje ovog cilja, uključujući i ocenu efikasnosti pravnih odgovora, primenjen je metodološki okvir koji kombinuje teorijski i praktični pristup, koji su zasnovani na kvalitativnoj analizi najvažnijih pranvih dokumenata i postojećih referenci o etici i politici sajber bezbednosti, kao i na praktičnim analizama stvarnih primera sajber incidenata. Očekivani ishod su preporuke za razvoj pravnih okvira na temeljima pravičnosti – uspostavljanju balansa između bezbednosnih potreba i etičkih principa. Ovakvim balansom bi se unapredilo poverenje građana u digitalne sisteme, a ujedno i ojačala bezbednost digitalnog društva.

Ključne reči: *privatnost, odgovornost, pravo, bezbednosni izazov, kritična infrastruktura*

5. REFERENCES

1. American Civil Liberties Union. (2001). *Surveillance under the USA/PATRIOT Act*. (2025, May 29) Retrieved from: https://www.aclu.org/documents/surveillance-under-usapatriot-act
2. California Legislature. (2020). *California Consumer Privacy Act, Cal. Civ. Code § 1798.100*. (2025, May 29) Retrieved from: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5&part=4.&chapter=&article=
3. Council of Europe. (2001). *Convention on Cybercrime (ETS No. 185)*. (2025, May 29) Retrieved from: https://www.coe.int/en/web/cybercrime/the-budapest-convention
4. Data Protection Commission. (2022). *Data Protection Commission announces decision in Instagram Inquiry*. (2025, May 30) Retrieved from https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-instagram-inquiry
5. DLA Piper. (2024). *Data protection laws in the United States*. (2025, June 2) Retrieved from: https://www.dlapiperdataprotection.com/index.html?t=law&c=US
6. Domazet, S., Marković, D. M., & Skakavac, T. (2024). Privacy under threat – The intersection of IoT and mass surveilance. *Pravo – teorija i praksa*, *41*(3), 109–124. DOI: 10.5937/ptp2403109D
7. Easterly, J., & Fanning, T. (2023, May 7). *The attack on Colonial Pipeline: What we've learned & What we've done over the past two years*. Cybersecurity and Infrastructure Security Agency (CISA). (2025, June 2) Retrieved from: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years
8. European Commission. (2023). *EU-US data transfers*. European Commission. (2025, June 2) Retrieved from: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en
9. European Commission**.** (2023). *Serbia 2023 Report (SWD(2023) 695 final)*. (2025, June 1) Retrieved from: https://enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_695_Serbia.pdf
10. European Parliament and Council. (2016). *Directive (EU) 2016/1148 on measures for a high common level of security of network and information systems across the Union*. (2025, June 1) Retrieved from: https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng
11. European Parliament and Council. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. (2025, May 30) Retrieved from: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
12. European Parliament and Council. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union*. (2025, May 29) Retrieved from: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
13. Federal Trade Commission. (2024). Equifax Data Breach Settlement. (2025, June 2) Retrieved from: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement
14. Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York: Doubleday
15. Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. New York: Metropolitan Books.
16. Marković, D. M., & Marković, D. (2025). Cybercrime and law – managing challenges and prospects in the digital age. *Pravo – teorija i praksa*, *42*(2), 49–61. https://doi.org/10.5937/ptp2502049M

17. Marković, D. M., & Zirojević, M. (2024). Izazovi u regulisanju i identifikaciji *deepfake* sadržaja [Challenges in regulating and identifying deepfake content]. U M. Počuča (Ur.), *Odgovori pravne nauke na izazove savremenog društva – zbornik radova sa naučnog skupa*. (str. 679–692). Novi Sad: Univerzitet Privredna akademija. DOI: 10.5937/PDSC24679M.
18. McGinnis, B. J., & Blaney, M. S. (2023). *European Commission adopts adequacy decision for EU-U.S. Data Privacy Framework.* National Law Review. (2025, June 2) Retrieved from: https://natlawreview.com/article/european-commission-adopts-adequacy-decision-eu-us-data-privacy-framework
19. Mladenov, M., & Stojšić Dabetić, J. (2021). Ažuriranje „prava da se bude zaboravljen" kao principa zaštite podataka u Evropskoj uniji [An update on the right to be forgotten as a principle of personal data protection in European union]. *Kultura polisa*, *18*(44), 99–109, DOI: 10.51738/Kpolisa2021.18.lr.2.04.
20. Partners Serbia. (2021). *Privacy and personal data protection in Serbia: An analysis of selected sectoral regulations and their implementation.* Partners for Democratic Change Serbia. (2025, June 2) Retrieved from: https://partners-serbia.org/public/documents/Privacy_and_Personal_Data_Protection_in_Serbia-_An_Analysis_of_Selected_Sectoral_Regulations_and_Their_Implementation,_PS.pdf
21. Schmitt, M., & Biller, J. (2017). *The NotPetya cyber operation as a case study of international law.* EJIL: Talk! (2025, June 2) Retrieved from: https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/
22. Schoenherr. (2023). *Rethinking EU-US personal data transfers and their effect on transfers from Serbia.* Schoenherr. (2025, June 2) Retrieved from: https://www.schoenherr.eu/content/rethinking-eu-us-personal-data-transfers-and-their-effect-on-transfers-from-serbia/
23. Standing Committee of the National People's Congress. (2017). *Cybersecurity Law of the People's Republic of China*. (2025, May 30) Retrieved from https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/
24. Stanford DigiChina. (2017). *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017).* (2025, May 29) Retrieved from: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/
25. Tidy, J. (2021, May 21). *Irish cyber-attack: Hackers bail out Irish health service for free.* BBC News. (2025, June 2) Retrieved from: https://www.bbc.com/news/world-europe-57197688
26. Zakon o informacionoj bezbednosti [Law on Information Security], *Službeni glasnik RS*, br. 6/2016, 94/2017 i 77/2019.
27. Zakon o zaštiti podataka o ličnosti [Law on the Protection of Personal Data], *Sl. glasnik RS,* br. 87/2018.
28. Zirojević, M., & Ivanović, Z. (2022). *Cyber Law – Serbia*. Belgrade: Institute of Comparative Law.
29.