UDK 34
ISSN (Štampano izd.) 0352-3713
ISSN (Online) 2683-5711

PRAVO

teorija i praksa

2 / 2025

PRAVO
teorija i praksa

Godina XLII **Novi Sad, 2025.** **Broj 2**

IZDAVAČ/PUBLISHER:
PRAVNI FAKULTET ZA PRIVREDU
I PRAVOSUĐE U NOVOM SADU
UNIVERZITET PRIVREDNA AKADEMIJA
Geri Karolja 1, 21000 Novi Sad
Tel.: 021/400-484, lokal 109; 021/400-499

SUIZDAVAČ/CO-PUBLISHER:
„PRAVO“ DOO
Novi Sad, Geri Karolja 1
21000 Novi Sad

Tehnička realizacija i štampa/Technical realization and print:
Feljton, Novi Sad

LAW
Theory and Practice

Year XLII **Novi Sad, 2025** **No. 2**

CIP – Katalogizacija u publikaciji
Biblioteka Matice srpske, Novi Sad

34

PRAVO : teorija i praksa = Law: Theory and Practice / glavni urednik Jelena Matijašević; odgovorni urednik Snežana Lakićević. – God. 1, br. 1 (1984)– . – Novi Sad : Univerzitet Privredna akademija, Pravni fakultet za privredu i pravosuđe u Novom Sadu : „Pravo" doo, 1984–. – 24 cm

Tromesečno.

ISSN 0352-3713

COBISS.SR-ID 5442050

LAW – Theory and Practice
Year XLII Novi Sad, 2025 No. 2

C O N T E N T S

PRAVO – teorija i praksa
Godina XLII **Novi Sad, 2025.** **Broj 2**

S A D R Ž A J

Tešović Olga[*]
https://orcid.org/0009-0005-3121-8752

UDK: 347.9:004.8
Original scientific paper
DOI: 10.5937/ptp2502001T
Received on: February 18, 2025
Approved for publication on:
May 14, 2025
Pages: 1–14

CONCEPTUALIZING JUDICIAL TRANSPARENCY AND PUBLIC TRUST – FRAMEWORKS FOR COMMUNITY-CENTERED JUSTICE

ABSTRACT: Judicial transparency and public trust represent the foundations of a functional rule of law and democratic governance. Transparency encompasses institutional openness, procedural clarity, and the public perception of fairness, forming the basis for accountability, equitable justice, and participatory governance. Despite growing global efforts, achieving substantive transparency remains a significant challenge for judicial systems. This paper examines the theoretical underpinnings of judicial transparency and trust, presenting a universal framework for integrating these principles into justice systems. Through a comparative analysis of global case studies, it identifies applicable strategies—including the use of emerging technologies such as artificial intelligence (AI) and blockchain—to improve transparency, enhance inclusivity, and address systemic inequalities. The findings show that transparent practices and participatory mechanisms strengthen public trust and inclusivity, offering practical guidance for future reforms.

Keywords: *judicial transparency, public trust, participatory governance, procedural justice, emerging technologies in justice.*

---

[*]LLD, Independent Research Associate, Belgrade, Serbia, e-mail: otolgates@gmail.com

1. Introduction

Judicial systems, as pillars of democratic societies, are entrusted with upholding the rule of law and delivering justice impartially. Their legitimacy hinges on the trust and confidence they inspire in the public. This legitimacy is not only derived from the formal authority vested in them but also from the perception of their integrity, transparency, and fairness (Tyler, 1990). However, in many societies, judicial systems face a crisis of trust fueled by perceived inefficiency, opacity, and systemic inequities (Mentovich, Prescott & Rabinovich-Einy, 2023).

Transparency in the judiciary serves multiple functions. It allows citizens to monitor and hold institutions accountable, understand judicial processes, and foster an informed dialogue on justice delivery. The conceptualization of transparency extends beyond merely providing access to information- it entails ensuring procedural clarity, institutional openness, and fostering a public perception that justice is accessible and fair (Bannister & Connolly, 2011). These facets collectively reinforce the legitimacy of judicial institutions (Ginsburg & Garoupa, 2015).

Despite growing global efforts to enhance transparency, many judicial systems face challenges such as inefficiency, corruption, and societal skepticism. For example, studies show that even in systems with procedural reforms, public trust often lags due to perceived inequities (Haavisto, 2002). This paper explores how judicial systems can address these challenges through conceptual models and practical mechanisms that embed transparency and public engagement.

2. Theoretical framework

Judicial transparency and public trust are deeply rooted in foundational theories of legitimacy, the public sphere, and participatory governance. These frameworks provide a comprehensive lens for understanding how judicial systems can achieve openness and accountability while fostering citizen trust and participation. In this section, we delve deeper into these theoretical underpinnings, exploring their relevance and interconnections within the judicial context.

2.1. Legitimacy theory

Legitimacy theory posits that the authority of institutions is contingent upon their acceptance by the governed. Tyler (1990) argues that this acceptance

hinges on perceptions of procedural justice rather than mere compliance through coercion. Procedural justice involves four key dimensions: fairness of decision-making, neutrality, respectful treatment of individuals, and trustworthiness of authorities. Institutions perceived as procedurally just are more likely to be viewed as legitimate and to foster voluntary compliance with their decisions.

In the context of judicial systems, legitimacy is closely tied to transparency. Transparent judicial processes allow the public to see how decisions are made, ensuring that they are based on objective criteria rather than favoritism or corruption (Ginsburg & Garoupa, 2015). For example, publishing court rulings, providing access to hearings, and explaining legal reasoning contribute to perceptions of fairness and impartiality.

Research also highlights the cyclical nature of legitimacy: public trust strengthens institutions, and strong institutions further reinforce trust (Mentovich, Prescott & Rabinovich-Einy, 2023). Thus, transparency serves both as a mechanism to build trust and as a signal of institutional commitment to fairness.

2.2. Public sphere theory

Habermas (1989) conceptualizes the public sphere as a domain where private citizens engage in rational-critical debate about public issues, shaping collective understanding and influencing institutional practices. Judicial transparency is pivotal in facilitating this discourse, providing citizens with the information necessary to evaluate and discuss the judiciary's performance.

Transparent judicial systems contribute to a vibrant public sphere by ensuring accessibility and openness in their operations. For example, livestreaming court proceedings or providing plain-language summaries of rulings enables citizens to participate meaningfully in dialogues about justice and legal reform (Fung, 2006). These practices demystify legal processes, reducing the perceived gap between legal authorities and the public.

Furthermore, Habermas emphasizes the bidirectional nature of transparency: it is not only about institutions disseminating information but also about being receptive to public input. This dynamic exchange strengthens the public's role as a check on judicial power and enhances the judiciary's responsiveness to societal needs.

2.3. Participatory governance

Participatory governance extends the principles of the public sphere by embedding citizen involvement directly into institutional decision-making

processes. Cornwall (2008) describes participatory mechanisms as tools to democratize institutions, making them more inclusive and responsive to diverse perspectives. In the judicial context, this might involve establishing advisory councils, creating forums for public consultations, or implementing participatory budgeting for legal aid services.

One of the most compelling aspects of participatory governance is its potential to address systemic inequities. Marginalized groups often face unique barriers in accessing justice, such as linguistic hurdles, socioeconomic disadvantages, or cultural stigmas. By actively involving these groups in the design and oversight of judicial practices, participatory governance ensures that transparency is coupled with equity and inclusivity (Fukuyama, 2014).

This framework also highlights the iterative nature of trust-building. Public engagement is not a one-time event but a continuous process of dialogue and adaptation. As citizens see their input reflected in institutional changes, trust deepens, creating a virtuous cycle of engagement and accountability.

2.4. Interconnectedness of frameworks

While legitimacy theory, public sphere theory, and participatory governance offer distinct insights, their interconnectedness is critical for a holistic understanding of judicial transparency and trust. Legitimacy provides the foundation for public trust; the public sphere facilitates discourse and scrutiny; and participatory governance operationalizes engagement into actionable practices.

For example, a judiciary that values legitimacy will prioritize procedural justice (Tyler, 1990) and openness to public discourse (Habermas, 1989). By incorporating participatory mechanisms (Cornwall, 2008), it ensures that transparency is not merely symbolic but genuinely responsive to societal needs. This synergy creates a robust framework for fostering trust and accountability in judicial systems.

3. Judicial transparency and its dimensions

Judicial transparency is foundational for enhancing accountability, promoting trust, and ensuring equitable access to justice. To fully understand its scope, it is vital to delve deeper into the nuances of its institutional, procedural, and perceptual dimensions. These dimensions offer a comprehensive framework for analyzing the judiciary's role in fostering democratic governance.

3.1. Institutional transparency

Institutional transparency concerns the systematic openness of judicial institutions in their structure, governance, and decision-making processes. It is the cornerstone of accountability, as it enables external actors-citizens, media, and civil society organizations-to evaluate the judiciary's performance.

Judicial independence is a key factor in maintaining public trust, as political interference in the judiciary undermines perceptions of fairness and impartiality. Research on Serbia's judiciary indicates that while institutional guarantees of independence exist, de facto implementation remains inconsistent, leading to judicial dissatisfaction and concerns about undue political influence (Dabetić, 2024).

Open access to court data, such as caseload statistics and judicial expenditures, strengthens public oversight. Studies show that countries with robust judicial data transparency tend to have higher perceived integrity in their judicial systems (Bannister & Connolly, 2011; Fukuyama, 2014).

Transparency in the appointment, promotion, and ethical oversight of judges can mitigate perceptions of bias or favoritism. Institutions like the Judicial Service Commission in South Africa publicly disclose appointment processes to ensure legitimacy (Judicial Service Commission, 2025).

Also, digital innovations, such as open-access judicial databases, amplify the judiciary's capacity for transparency. The European Court of Human Rights provides an online case-law database, HUDOC, which exemplifies institutional transparency on an international scale (European Court of Human Rights, 2025).

Emerging technologies like blockchain offer innovative tools for ensuring institutional accountability. Blockchain's decentralized and tamper-proof ledger system can enhance transparency in judicial operations, such as recording judgments, case filings, and court expenses. For example, courts could use blockchain to maintain publicly accessible and immutable records of judicial proceedings, fostering trust in institutional integrity (Bannister & Connolly, 2011).

Institutional transparency often encounters resistance due to concerns over judicial independence. Balancing openness with the judiciary's need to operate free from undue influence remains a critical challenge.

3.2. Procedural transparency

Procedural transparency emphasizes the clarity, accessibility, and predictability of legal processes. It directly influences public perceptions of fairness and inclusivity in judicial systems.

Many legal systems are criticized for their complex and technical language, which alienates the public. Initiatives like "plain language judgments," implemented in New Zealand courts, make judicial decisions more accessible to non-specialists (Fung, 2006).

Virtual hearings and e-filing systems are also important. The COVID-19 pandemic accelerated the adoption of virtual court hearings and electronic filing systems. These digital tools not only increase procedural transparency but also reduce barriers for individuals who cannot physically attend court proceedings (Mentovich, Prescott & Rabinovich-Einy, 2023).

The widespread shift to remote court proceedings during the pandemic has raised critical legal and ethical questions, particularly concerning fair trial rights, technological limitations, and judicial efficiency. Studies on remote trials emphasize the need to balance efficiency with procedural safeguards, ensuring that digital solutions do not compromise due process or access to justice (Krstić, Tešović, Milovanović & Dakić, 2021). A comparative analysis of international standards in remote judging further highlights the importance of maintaining procedural fairness and aligning virtual court practices with probation systems to ensure equitable legal outcomes (Tešović, 2024a).

Procedural transparency focuses on ensuring that judicial processes are clear, accessible, and predictable. AI-powered tools are increasingly being used to demystify legal processes. For instance, AI-driven chatbots and virtual assistants can guide users through court procedures, explain legal jargon, and provide updates on case statuses. These tools not only reduce barriers to justice for individuals unfamiliar with legal systems but also streamline communication between courts and the public (Mentovich, Prescott & Rabinovich-Einy, 2023).

Furthermore, AI's predictive analytics capabilities can assist courts in managing caseloads by identifying bottlenecks and suggesting resource allocation strategies. Virtual court platforms, accelerated during the COVID-19 pandemic, combine AI with video conferencing to enable remote hearings. This not only improves procedural efficiency but also expands access for geographically and economically marginalized populations.

Procedural transparency also involves educating the public about their legal rights. In India, legal literacy programs have been launched to empower marginalized communities with knowledge of procedural law.

Ensuring procedural transparency requires resources, training, and technological infrastructure, which may be limited in developing judicial systems. Additionally, overemphasis on procedural reforms without addressing deeper systemic inequities can lead to disillusionment among the public.

3.3. Perceptual transparency

Perceptual transparency focuses on the public's trust in the judiciary's commitment to openness and fairness. It is shaped not only by direct experiences but also by societal narratives and media representation.

Transparency in legal processes must be balanced with confidentiality to maintain trust in the justice system. The principle of lawyer-client confidentiality is fundamental in ensuring fair representation and upholding the right to a fair trial. European legal frameworks emphasize that any breach of this confidentiality could compromise both procedural justice and public confidence in the legal system (Bingulac & Miljenović, 2021).

Media play a crucial role in shaping public perceptions of judicial transparency. While constructive reporting can enhance public understanding, sensationalist media coverage often distorts the image of the judiciary and erodes trust. For instance, media coverage of corruption scandals often overshadows broader transparency initiatives (Cornwall, 2008). Legal frameworks must balance transparency with safeguards to protect procedural integrity and the presumption of innocence (Tešović, 2024b).

Engaging communities through town halls, public consultations, and participatory forums helps address misconceptions about the judiciary and enhances perceptual transparency. Cultural contexts shape how transparency is perceived. In collectivist societies, for example, judicial transparency might be evaluated more through outcomes benefiting the community than through procedural openness (Fukuyama, 2014).

Changing public perceptions requires sustained effort and alignment between rhetoric and practice. Transparency initiatives that fail to deliver tangible improvements in access or equity risk being perceived as performative.

4. Comparative analysis: judicial transparency and engagement across contexts

A comparative analysis of judicial transparency and engagement reveals diverse strategies adopted globally to address systemic challenges and strengthen public trust. By examining key examples across regions, this section highlights successes, challenges, and lessons learned, demonstrating how transparency and community participation can be tailored to specific legal, cultural, and social contexts.

4.1. North America: open court principles and technology integration

In North America, judicial systems have long prioritized the principle of open courts, which underpins public trust and accountability. The United States exemplifies this approach through its emphasis on access to judicial information. The Public Access to Court Electronic Records (PACER) system provides online access to federal court documents, facilitating transparency by allowing individuals to track case progress and review court decisions. However, its subscription-based model has drawn criticism for limiting access for low-income populations, highlighting the need for equitable transparency mechanisms (Bannister & Connolly, 2011). Additionally, livestreaming high-profile court cases has expanded public engagement, although sensationalist media coverage occasionally distorts public perceptions and undermines trust (Habermas, 1989). Balancing openness with judicial independence remains a critical challenge.

Canada has advanced transparency and accessibility through initiatives such as the Canadian Legal Information Institute (CanLII), which offers free online access to judicial decisions, statutes, and regulations. This institutional transparency is complemented by proactive judicial outreach programs. Canadian judges regularly engage with the public through lectures, school visits, and seminars, demystifying judicial processes and fostering trust. The Canadian model demonstrates that transparency efforts must combine open access to legal information with direct community engagement to be truly effective (Cornwall, 2008).

4.2. Europe: institutional reforms and public participation

In Europe, Finland provides a notable example of how procedural reforms can enhance judicial transparency and engagement. Finland's comprehensive judicial reform in 1993 introduced principles of orality, immediacy, and concentration to improve transparency and efficiency. Orality emphasized verbal communication during hearings, fostering direct interaction between judges, parties, and witnesses. The principle of immediacy ensured that judicial decisions were based solely on evidence presented in the main hearing, while concentration streamlined proceedings into uninterrupted sessions. These reforms reduced procedural delays, improved public understanding of judicial processes, and enhanced trust in the judiciary (Haavisto, 2002).

Finland also prioritized community participation through preliminary hearings and lay judge systems, encouraging informal dialogue and public

representation in decision-making. However, cultural resistance among legal professionals and limited technological infrastructure initially posed challenges to implementation. Over time, training and consistent adaptation of procedures ensured the reforms' success, highlighting the importance of aligning judicial transparency initiatives with cultural and institutional contexts. Finland's experience demonstrates the effectiveness of participatory approaches in enhancing procedural fairness and building trust.

On the other hand, Estonia represents a technology-driven approach to judicial transparency. Its e-Court system enables citizens to access case progress, submit filings electronically, and participate in virtual hearings. Additionally, the judiciary publishes anonymized case data to promote transparency while protecting privacy. However, digital literacy and infrastructure gaps among rural and elderly populations underscore the importance of addressing the digital divide to ensure equitable access (Fukuyama, 2014).

The United Kingdom integrates institutional transparency with grassroots engagement. Judicial annual reports provide detailed insights into court performance and reforms, ensuring accountability. Community panels in magistrate courts incorporate public input into sentencing practices, bridging the gap between judicial authorities and citizens. The U.K. example underscores that combining institutional transparency with participatory governance fosters trust and accountability (Fung, 2006).

4.3. Asia: tradition and innovation in judicial transparency

In Asia, India's judiciary has embraced innovative practices to improve transparency and engagement. Landmark cases are livestreamed from the Supreme Court, ensuring public access to critical judicial proceedings. Additionally, Lok Adalats, or People's Courts, provide accessible and affordable dispute resolution mechanisms that prioritize community involvement. Despite these advancements, persistent delays and backlogs in traditional courts erode trust, highlighting the need for broader procedural reforms (Bobocel & Gosse, 2015).

Japan's judiciary exemplifies the integration of transparency with cultural sensitivity. The Saiban-in system, introduced in 2009, involves lay judges in criminal trials, promoting public participation and trust. Public outreach programs, including judicial lectures and exhibitions, enhance legal literacy and demystify judicial processes. Japan's experience demonstrates that transparency initiatives must respect cultural norms to avoid resistance and ensure meaningful engagement (Beier, Eib, Oehmann, Fiedler & Fiedler, 2014).

4.4. Africa: grassroots engagement and localized approaches

In Africa, Kenya's Judiciary Transformation Framework (2012–2016) illustrates the power of integrating transparency and community engagement. Performance management tools evaluate courts using transparent metrics, while Court Users Committees bring together judicial officers, civil society, and citizens to address systemic challenges. However, political interference and limited resources remain significant obstacles to sustaining these initiatives (Cornwall, 2008).

Rwanda's Abunzi mediation committees provide a grassroots model for judicial engagement. Community-elected mediators resolve disputes locally, reducing reliance on formal courts and fostering public trust. By emphasizing dialogue and cultural relevance, the Abunzi system addresses systemic inequities and enhances access to justice. Rwanda's experience highlights the effectiveness of decentralized, community-driven models in building trust and addressing resource constraints (Fukuyama, 2014).

4.5. Latin America: transparency in post-conflict societies

Latin American countries such as Colombia and Brazil have leveraged judicial transparency to address systemic inequities and rebuild trust in post-conflict contexts. In Colombia, Peace and Reconciliation Courts integrate restorative justice principles, prioritizing public participation to heal societal divisions. Open Justice Platforms provide real-time access to judicial proceedings, promoting accountability and transparency. However, ensuring judicial safety and impartiality in politically sensitive cases remains a critical challenge (Mentovich, Prescott & Rabinovich-Einy, 2023).

In Brazil, Public Defender's Offices facilitate legal representation for marginalized groups and host community dialogues to enhance engagement. Digital access to court records reduces procedural delays and promotes institutional transparency. These initiatives demonstrate the importance of addressing systemic inequities through participatory and transparent practices, fostering trust among historically underserved communities (Bannister & Connolly, 2011).

4.6. Key insights from comparative analysis

Judicial transparency and engagement are essential for fostering trust and accountability, but their implementation must be tailored to each region's unique socio-political and cultural context. Technology serves as a powerful

enabler of transparency but requires substantial investment in infrastructure and digital literacy to bridge equity gaps. Balancing judicial independence with openness is critical to maintaining impartiality while enhancing accountability. Finally, grassroots and community-driven approaches, such as Finland's participatory hearings or Rwanda's Abunzi committees, underscore the importance of culturally relevant and localized solutions in addressing systemic barriers and building trust.

This comparative analysis demonstrates that while the principles of transparency and engagement are universal, their successful application depends on nuanced strategies that respect local contexts and priorities.

5. Conclusions and future directions

Judicial transparency and public trust are foundational to the legitimacy and effective functioning of legal systems. This analysis has demonstrated that transparency not only enhances accountability and procedural fairness but also reinforces public confidence in judicial institutions. Trust, in turn, sustains public engagement and institutional legitimacy, creating a positive feedback loop (Tyler, 1990).

To ensure the success of transparency and engagement initiatives, reforms must align with local socio-political contexts and address systemic barriers. Institutional transparency can be strengthened through clear policies and open data practices, while procedural reforms, such as simplifying legal language and adopting alternative dispute resolution mechanisms, improve accessibility (Fukuyama, 2014). Equally important is perceptual transparency, which requires ongoing efforts to align public perceptions with judicial realities through outreach and inclusive dialogue (Cornwall, 2008).

Emerging technologies, such as artificial intelligence (AI) and blockchain, present transformative opportunities for judicial transparency. AI tools can streamline case management, provide predictive analytics to support decision-making, and improve public access to legal information through automated systems. For example, AI-driven chatbots could answer basic legal questions and assist users in navigating judicial procedures (Mentovich, Prescott & Rabinovich-Einy, 2023). Blockchain technology, on the other hand, can enhance accountability by creating tamper-proof records of judicial decisions and proceedings, ensuring integrity and transparency (Bannister & Connolly, 2011). However, these technologies also raise concerns about data privacy, algorithmic bias, and equitable access, underscoring the need for robust governance frameworks and ethical guidelines (Habermas, 1989).

Future research should focus on the intersection of technology and judicial transparency, exploring how innovations like AI and blockchain can be harnessed responsibly to enhance trust and efficiency. Comparative studies across diverse legal systems can uncover best practices and common challenges, particularly in addressing systemic inequities (Bobocel & Gosse, 2015). Moreover, interdisciplinary approaches that integrate legal, technological, and sociological perspectives are critical to designing inclusive and effective transparency initiatives.

In envisioning the future, embedding transparency and engagement into judicial systems is not merely a reform but a transformation. By leveraging innovation, fostering inclusivity, and prioritizing trust, judicial systems can strengthen their legitimacy and ensure that justice is accessible, fair, and responsive to all members of society. Achieving this vision requires sustained commitment and collaboration across legal, technological, and community stakeholders.

Tešović Olga
Naučni saradnik, Beograd, Srbija

KONCEPTUALIZACIJA SUDSKE TRANSPARENTNOSTI I JAVNOG POVERENJA – OKVIRI ZA PRAVOSUĐE USMERENO KA ZAJEDNICI

APSTRAKT: Sudska transparentnost i javno poverenje predstavljaju temelje funkcionalne vladavine prava i demokratskog upravljanja. Transparentnost obuhvata institucionalnu otvorenost, proceduralnu jasnoću i percepciju pravičnosti u javnosti, čineći osnovu za odgovornost, pravičnu pravdu i participativno upravljanje. Uprkos rastućim globalnim naporima, postizanje suštinske transparentnosti i dalje ostaje izazov za pravosudne sisteme. Ovaj rad ispituje teorijske osnove sudske transparentnosti i poverenja, predstavljajući univerzalni okvir za integrisanje ovih principa u pravosudne sisteme. Kroz komparativnu analizu globalnih studija slučaja, identifikuju se primenljive strategije, uključujući korišćenje savremenih

tehnologija poput veštačke inteligencije (AI) i blokčejna, u cilju unapređenja transparentnosti, jačanja inkluzivnosti i rešavanja sistemskih nejednakosti. Nalazi pokazuju kako transparentne prakse i participativni mehanizmi jačaju poverenje i inkluzivnost, nudeći praktične smernice za buduće reforme.

Ključne reči: *sudska transparentnost, javno poverenje, participativno upravljanje, proceduralna pravda, savremene tehnologije u pravosuđu.*

References

1. Bannister, F., & Connolly, R. (2011). The Trouble with Transparency: A Critical Review of Openness in e-Government. *Policy & Internet*, *3*(1), pp. 1–30. DOI: http://doi.org/10.2202/1944-2866.1076
2. Beier, S., Eib, C., Oehmann, V., Fiedler, P., & Fiedler, K. (2014). Influence of Judges' Behaviors on Perceived Procedural Justice. *Journal of Applied Social Psychology*, *44*(1), pp. 46–59. DOI: https://doi.org/10.1111/jasp.12199
3. Bingulac, N., & Miljenović, D. (2021). Lawyer Confidentiality. *Pravo – teorija i praksa, 38*(3), pp. 42–52. DOI: https://doi.org/10.5937/ptp2103042B
4. Bobocel, D. R., & Gosse, L. (2015). Procedural justice: A historical review and critical analysis. In: Cropanzano R. S., & Ambrose M. L. (eds.), *The Oxford handbook of justice in the workplace*. (pp. 51–87). New York: Oxford University Press, DOI: https://doi.org/10.1093/oxfordhb/9780199981410.013.3
5. Cornwall, A. (2008). Unpacking 'Participation': Models, Meanings and Practices. *Community Development Journal*, *43*(3), pp. 269–283. DOI: https://doi.org/10.1093/cdj/bsn010
6. Dabetić, V. (2024). Independence of the Judiciary as a Path and a Goal – The Voice of the Profession. *Pravo – teorija i praksa, 41*(2), pp. 57–75. DOI: https://doi.org/10.5937/ptp2402057D
7. European Court of Human Rights (2025). HUDOC case-law database. Downloaded 2025, January 25 from https://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC
8. Fukuyama, F. (2014). *Political Order and Political Decay: From the Industrial Revolution to the Globalization of Democracy*. New York: Farrar, Straus and Giroux

9. Fung, A. (2006). Varieties of Participation in Complex Governance. *Public Administration Review*, *66*, pp. 66–75. Downloaded 2025, January 25 from http://www.jstor.org/stable/4096571?origin=JSTOR-pdf
10. Ginsburg, T., & Garoupa, N. (2015). *Judicial Reputation: A Comparative Theory*. Chicago: University of Chicago Press
11. Habermas, J. (1989). *The Structural Transformation of the Public Sphere*. Cambridge: MIT Press
12. Haavisto, V. (2002). *Court Work in Transition: An Activity-Theoretical Study of Changing Work Practices in a Finnish District Court – academic dissertation*. Helsinki: University of Helsinki
13. Judiciary Transformation Framework (Kenya) (2012–2016). Judiciary of Kenya. Downloaded 2025, January 25 from https://kenyalaw.org/kl/fileadmin/pdfdownloads/JudiciaryTransformationFramework.pdf
14. Judicial Service Commission (2025). *About the JSC*. Downloaded 2025, January 25 from https://www.judiciary.org.za/index.php/judicial-service-commission/about-the-jsc
15. Krstić, I., Tešović, O., Milovanović, I., & Dakić, D. (2021). *Remote Trials: Legal Framework and Practice.* Belgrade: Forum of Judges of Serbia
16. Mentovich, A., Prescott, J. J., & Rabinovich-Einy, O. (2023). Legitimacy and Online Proceedings: Procedural Justice, Access to Justice, and the Role of Income. *Law & Society Review*, *57*(2), pp. 189–213. DOI: https://doi.org/10.1111/lasr.12653
17. Tešović, O. (2024a). Evaluating International Standards in Remote Judging: Comparative Analyses and the Intersection with Probation Practices. In: Tomita. M. & Ungureanu. R. (eds.), *Proceedings of the 8th International Conference "Designing the Future of Criminal Justice System Under the Lens of Technology"*, (pp. 132–138). Timisoara: Univeristatea de Vest de Timisoara, Romania, DOI: http://doi.org/10.26352/I516-SPECTO-2024
18. Tešović, O. (2024b). Transparency of Criminal Proceedings and the Media: Principle, Limits, and Challenges. In: Kostić, J. & Matić Bošković, M. (eds.), *VIII International Scientific Conference – Media, Criminal Law, and Judiciary: Thematic Collection of Papers of International Importance.* (pp. 167–178). Belgrade: Institute of Comparative Law; Institute of Criminological and Sociological Research
19. Tyler, T. R. (1990). *Why People Obey the Law*. Princeton, NJ: Princeton University Press

Golić Darko[*]
https://orcid.org/0000-0003-2315-5040

UDK: 352
Original scientific paper
DOI : 10.5937/ptp2502015G
Received on: April 26, 2025
Approved for publication on:
May 23, 2025
Pages: 15–35

THE ROLE OF ADMINISTRATIVE DISTRICTS IN THE ADMINISTRATIVE SYSTEM OF SERBIA

ABSTRACT: This paper analyzes the role of administrative districts and local units of state administration authorities, as well as the needs and possibilities for their reform. The non-central aspect of public administration itself constitutes a complex whole with multiple distinct elements, interrelations, and needs. In this context, the paper examines the possibilities and methods for *"strengthening administrative districts"* and *"improving vertical and horizontal oversight in the execution of original and delegated tasks"* at the non-central level, as defined by current planning documents. The core of this analysis is grounded in positive legal provisions, as well as strategic and planning documents in Serbia, accompanied by relevant comparative references. The main research dilemma concerns the limited possibilities for enhancing the performance of state administrative tasks through or within administrative districts. This limitation stems from the nature of the non-central aspect of public administration as a complex subsystem with two components: local self-government with its own original tasks (decentralized aspect), and local self-government with delegated tasks alongside local units of state administration authorities (more or less centralized aspect), which are interconnected through the administrative district.

[*]LLD, Full Professor, University Business Academy in Novi Sad, Faculty of Law for Commerce and Judiciary in Novi Sad, Novi Sad, Serbia, e-mail: g.darko83@gmail.com

Keywords: *administrative district, deconcentration, head and council of the administrative district.*

1. Introduction

Starting from the assumption that non-central performance of certain state administrative tasks can be improved, and that a quality system of oversight over the performance of delegated tasks to local self-government units and their coordination is a prerequisite for fulfilling the responsibilities of local self-government, this paper addresses the possibility of legally improving the role of administrative districts, and the relationship between local self-government units and regional branches of state administration. The adopted strategic and planning documents express a commitment to expanding the role of administrative districts, particularly through improving the system of oversight over the implementation of delegated tasks.

In theory, despite certain terminological inconsistencies, but without essential disagreements in the qualification of these phenomena, a distinction is made between the mentioned relationships. The transfer of state tasks to existing territorial-political units is referred to as decentralization, which, if referring only to the delegation of state administrative tasks, can be termed administrative decentralization, as its lower level, in contrast to the creation of lower (regional) authorities or units, which represents a form of deconcentration.[1] Deconcentration, too, can be a form of mitigating centralization. By nature, administrative districts are a form of "pure deconcentration," and their significance primarily stems from the importance

[1] Marković (2015, p. 403) denies the connection between decentralization (including administrative), which implies the transfer of state administration tasks to local self-government bodies, and not to lower bodies appointed by the state (deconcentration). Tomić (2016, p. 155) considers administrative decentralization – deconcentration to mean the transfer of tasks to regional state bodies or regional units of state bodies ("the hierarchical scale is truncated"), and true decentralization implies a certain degree of autonomy (organizational and functional) in precisely defined administrative tasks, with the proviso that in terms of self-government bodies, there may be an overlap (self-governing and entrusted tasks) of these two phenomena. Vlatković and Golić (2021, p. 61), similarly to Marković, defines decentralization as the transfer of state administration tasks to entities outside the same organizational structure and subordination, in contrast to deconcentration, which implies the transfer of decision-making from higher authorities to bodies or units of a hierarchically lower level. Pusić (2002, p. 83) also considers decentralization to include any form of transfer of administrative tasks from the state to organizations outside its organizational system or that are at least under weaker central influence. The relevance of this distinction concerns the qualification of entrusted tasks, which, in our opinion, would fall under administrative decentralization.

of the local units of state administration. Although the role of these local units is defined by the Law on State Administration (2005), with the possibility of expansion, it is essential to bear in mind that the administrative district does not represent a separate level of government. The elements and character of the territorial organization of the Republic of Serbia derive from the Constitution, and introducing special entities within the administrative-territorial system, with the aim of territorially unifying non-central tasks, is particularly delicate, especially regarding the definition of their role.

Considering the content and types of state administration work, the internal organization of its bodies, and the nature of administrative districts, the issues that require analysis relate to the role of regional units of state bodies, and the role of the administrative district as a form of unification, cooperation, and coordination. An important limitation relates to the constitutional determinants of the territorial organization of the Republic, that the administrative district is not a territorial-political unit, and can only be a matter of the internal organization of the state administration.

In this regard, it is necessary to address several issues, namely: 1) the legal nature of the administrative district; 2) the legal definition of regional units of state administration; 3) harmonization of relations between non-central units in a given system of administrative-territorial organization; 4) oversight of delegated tasks performed by local self-government units.

2. Strategic and planning documents

The objectives set out in the valid strategic and planning documents determine the function of this paper. They arise from an analysis of the state of the administrative system and the weaknesses of the institutional framework. Moving from the most general to the more specific and concrete, these documents ultimately aim for a more efficient public administration, with good governance and quality public services, without changing the system of state administration or local self-government, which the constitutional framework does not permit. They foresee reform measures across various elements of the administrative-territorial system, primarily in the performance of delegated tasks.

Public Administration Reform Strategy in the Republic of Serbia for the period 2021-2030 (2021) cites as one of its goals the "development of a modern, professional, efficient, and responsible local self-government that is capable of providing quality public services to citizens and the economy, applying the principles of good governance in its work, improving the quality

of life of citizens, and contributing to the balanced development of the Republic of Serbia." It states that an improved local self-government system implies redefining its position and applying the principles of subsidiarity and citizen participation in managing public affairs, developing its capacities and organizational improvements, a sustainable financing system, long-term planning and the promotion of local development, efficiency of local administration and public services, the quality and availability of their services, enhancement of inter-municipal cooperation, and coordination among different levels of public authority in joint management of public affairs.

The Local Government Reform Program, as an integral part of the Strategy, represents a political and planning framework for the development of the local self-government system and for preparing other public policy documents, laws, by-laws, and development projects aimed at "developing the local self-government system in line with the adopted vision, goals, and reform measures contained in this program."

Local Self-Government System Reform Program of the Republic of Serbia (2021–2025) includes a segment titled "Relations between the Republic and Provincial Authorities and Local Self-Government Authorities." This part particularly emphasizes strengthening the role of the administrative district. It notes that higher levels of government do not exercise their preventive and advisory functions, "but instead rely on the detection of committed illegalities or irregularities and their sanctioning. Administrative districts, therefore, have not been sufficiently utilized, as not all state administrative tasks that could be carried out in this manner and brought closer to citizens have been delegated to them." However, they cannot compensate for the absence of a middle level of government, which has existed since the abolition of inter-municipal regional communities in 1990. The coordination function of the administrative district is also insufficiently developed. The administrative district, it is stated, can be one of the key mechanisms for developing a national system of oversight and inspection, which would act to ensure legality and positively guide lower levels of government. "Administrative districts could contribute to easing the burden on republic-level authorities and increasing work efficiency. Quality monitoring would allow state authorities to detect problems in a timely manner and undertake measures to overcome them."

The Action Plan 2021–2023, as part of the Program, emphasizes elements that should be redefined. Regarding the improvement of vertical and horizontal oversight in the performance of original and delegated tasks (Measure 1.6), it is stated that a quality oversight system is a prerequisite for the effective

fulfillment of local responsibilities. For this issue, the so-called third level of reform (pp. 129–130) is particularly relevant, which entails the enhancement of the supervisory function of state administration. As a priority, it mentions the redefinition of the role of administrative districts and the regional units of ministries toward better realization of oversight over the performance of delegated tasks, with the potential functional strengthening of the districts as the core oversight system in this area.

From the provisions of the planning documents cited above, no clear conclusion can be drawn as to when a specific goal or measure refers to the administrative district and when to the regional units of state authorities established for its territory, especially concerning the issue of oversight.

3. Legal nature of administrative districts

The Republic of Serbia is a unitary state, and state authority is limited by the citizens' right to territorial autonomy and local self-government, which is subject only to constitutional and legal oversight (Article 12 of the Constitution). The territorial organization of Serbia includes local self-government units and autonomous provinces as a form of territorial autonomy, which may be entrusted with certain tasks of state administration.[2] Decentralized units are public law entities, with original and delegated competences,[3] different legal regimes, limited rights to self-organization, directly elected authorities,

[2] Germany, as a federal state, does not have its own regional administrative bodies. Administrative tasks are mainly carried out by the provinces, under whose competence is the local self-government system. In this regard, there is no uniform system – sometimes it is one-tier, sometimes two-tier (municipality and district), sometimes mixed, some cities also have the status of a district, and associations of municipalities also have great importance in the administrative system. Berlin, as a federal unit, is divided into several administrative districts as a form of deconcentration. Decentralized units also carry out the entrusted competencies of the provincial administration, primarily districts, which are also units of deconcentrated provincial administration, thus combining the double and single track (mostly).

[3] In Hungary, the socialist model of centralization and deconcentration was changed in favor of decentralization. Its units are municipalities and counties (mixed system), with mandatory, optional and delegated competencies, they are not in a hierarchical relationship, while decentralized forms of state administration (districts, decos, district commissioners) have been continuously weakened or eliminated in favor of decentralization, where counties have become decentralized units, and regions are forms of their connection. The situation is similar in the Czech Republic, with two-level, polytypic decentralization, where the compentencies of the former district administration have been transferred to individual municipalities or regions. However, the state ministry gives its consent to the election of the heads of administrative authorities. (Vučetić, 2012, pp. 301–304. and p. 308).

general legal acts, revenues, property, and means of protection (Lapčević & Rapajić, 2023, pp. 112–137).

Within the administrative-territorial system since 1992, administrative districts have existed as institutions primarily linked to the state (Marković, 2015, p. 433). Their existence is justified by the fact that not all state administration tasks can be performed at the headquarters of the authority; thus, some tasks are physically relocated to bring administrative power closer to citizens. Therefore, state administration authorities establish their regional units to perform certain tasks outside their headquarters. However, the territorial jurisdiction of regional authorities is not left to the discretion of each authority individually. The Government, as the holder of executive power, establishes administrative districts and determines their territories.

According to the Law on State Administration (2005, Article 38): "An administrative district is established for performing tasks of state administration outside the headquarters of the state administration authority." They are established by Government decree, which also determines their territories and seats, as well as *the conditions under which regional units for two or more administrative districts, one or more municipalities, a city or an autonomous province may be established*. Therefore, an administrative district is a part of the territory of the Republic for which regional units of state administration bodies are mainly formed. The original term – "districts" – were supposed to be some form of substitution of inter-municipal communities from the socialist constitutionalism (1974), *but they were not*. As a constitutional category in the communal system, they represented a de facto higher level of government, a mandatory association of municipalities, with original and entrusted compentancies, including normative, executive, planning, administrative, with their own assemblies, administration, public services, general acts, and encompassed much more than what regional units or administrative districts represent today as a form of harmonization of relations (Borković, 1981, pp. 172–175). Without disputing the fact of the conceptual difference in the structure of the administrative system and the local government, some of the positive achievements and experiences of these communities were easily abandoned, essentially mimicking rigid deconcentration. The existing territorial organization also serves as the territorial basis for deconcentration, which is a kind of standard in comparative law. They are not a constitutional category but an element of the internal organization of state administration, prescribed by law, with their establishment falling under the jurisdiction of the Government. They do not possess legal personality, competences, elected bodies, revenues, or independent existence; rather, certain tasks of

state administration are performed within them. Hence, they are forms of administrative deconcentration (Marković, 2015, p. 435). Petrović (2006, p. 202) emphasizes the essential difference between decentralization and deconcentration in the fact that in deconcentration, central authorities independently appoint and dismiss officials of lower administrative units (personal authority), while in the second case, this right belongs to the citizens of the narrower units. Kostić (2000, p. 107) states that in the Administrative Law of the Kingdom of Yugoslavia deconcentration represented a mitigated form of centralization, where a certain range of competencies was transferred for final resolution to lower state bodies, closer to the people. They are appointed, not elected, hierarchically subordinate, not simply under the control of higher bodies, the acts they adopt cannot be modified by higher bodies. The current Decree on Administrative Districts establishes 29 administrative districts.

The nature of this institution can be observed (and supplemented) through its bodies. The Head of an administrative district is an official appointed and dismissed by the Government for a four-year term, upon the proposal of the minister responsible for administrative affairs, to whom he or she reports. The head "coordinates the work of regional units, monitors the implementation of directives and instructions issued to them; monitors the implementation of work plans of regional units and ensures the conditions for their work; monitors the work of employees in regional units and proposes initiation of disciplinary proceedings against them; cooperates with regional units not established for the district area; cooperates with municipalities and cities and performs other duties determined by law" (Article 40). The head of an administrative district is not the head of a regional administration. Full seniority is a historical relic, e.g. of the great prefect or ban during the Kingdom, earlier of the French prefect, Russian governor, etc., incompatible with the tendency towards professionalization. Considering his duties and powers, a conclusion can be drawn about a non-hierarchical, coordinating, initiating and conditionally supervisory role, in which respect a certain expansion may occur – to complete and specify the issue of coordination and supervision ("monitoring implementation"), but the character of this function cannot be changed into a decision-making or a function with independent powers, because it is linked to the administrative district as a derived, coordinating and non-political institution. The head manages the professional service, which provides him with professional and technical support, prescribes its internal organization with the consent of the Government, and decides on the rights and obligations of its employees. Supervision over the purposefulness of its work is carried out by the Ministry of Administration. The non-hierarchical, coordinating role

of the Head is also visible through the role of the professional service, which is responsible for tasks common to all regional units of state administration within the district.

Although the administrative district is primarily a state institution, this statement is not absolute. While this is its predominant feature, the nature and potential functions of the district can also be viewed from the perspective of its bodies, especially the District Council. The Council consists of the District Head and the presidents of municipalities and mayors from the District's area."The Council coordinates relations between regional units of state administration and municipalities and cities within the administrative district and proposes measures for improving the work of the district and its regional units" (Article 42). Its modus operandi is regulated by decree. It is, therefore, a form of institutionalized cooperation between non-central administrative-territorial units — local self-governments and regional administration, embodied in the District Head. The Head convenes and chairs Council sessions, which must be held at least once every two months. Sessions may also be convened at the request of two-thirds of the Council members. The Council adopts decisions by a majority vote of all its members, suggesting that participation of local self-government units in this body would not be merely symbolic if the Council had a relevant role. The administrative district may thus represent a form of integration, harmonization, and cooperation between regional units of state administration and local self-government units, and not merely a territory for which regional units are established. The legal formulation of "harmonizing relations," as the only possible one in line with the legal nature of the district, gains relevance depending on practice, political will, needs and initiative of involved actors, and also the normative clarification of this role and its implementation methods.

Conditionally, administrative districts could represent a form of functional – *administrative regionalization*. In theory, regionalization is viewed primarily through political content. It is based on economic, social, traffic, and cultural criteria that make an area more compact, more homogeneous (as opposed to deconcentration, which is based primarily on the need for more effective performance of administrative tasks). The Government determines the area of an administrative district so that it enables rational and effective work of regional units of state administration (more about the nature of administrative districts in: Milkov, 2009, p. 137). Still, any unification of administrative tasks at a level broader than basic local units, based on flexible criteria ("rational and efficient" are not strict), which along with administrative goals includes broader objectives or interests, may represent a form of functional regionalization,

which serves regional needs without establishing a new level of government.[4] Functional regionalization, in addition to the number, significance, and diversity of administrative tasks, is also conditioned by the concept of single-tier, monotypic local self-government. A very similar system of local governments (until the establishment of regions), with original and delegated competencies, supervision, but also districts, as well as regional units of state administration, i.e. deconcentration, exists in Slovenia. Administrative districts may provide a basis for broader inter-municipal cooperation, harmonization of relations with regional administration, development planning, oversight, and serve as a starting point for its functional enhancement.

The District Council also functions as a form of inter-municipal cooperation and collaboration with regional units of state administration. To some extent, the District Council could substitute the functions of second-tier self-government, i.e., provide a minimal democratic legitimacy for regional administration. This characteristic was expressed to a greater extent during the direct election of the municipal president. However, without denying the potential of district councils to initiate and encourage inter-municipal and their role remains declarative due to a lack of good practice, tradition of cooperation, and structural weaknesses in most municipalities. Therefore, through appropriate amendments to the Law and Decree, the role of district councils *in harmonizing local policies and development programs, in launching initiatives, operational coordination, in encouraging the integration of local services or bodies, introducing a certain supervisory function,* etc. should be expanded and specified. Especially in the field of planning economic development, infrastructure, civil protection, water supply, environment, waste management, tourism development, etc. (Golić, 2014, pp. 148–150). The cooperation that is envisioned through district councils should be more specifically defined, somewhat more substantive, but without the ambition

[4] Marković (2015, p. 436) considers it incorrect to understand that administrative districts can be a means of regionalization, because administrative deconcentration is carried out on different criteria compared to regionalization, which is carried out according to geographical, economic, cultural, demographic and other factors that ensure a relatively homogeneous community. Respecting the distinction between these concepts, our understanding of functional, non-political regionalization is somewhat broader, encompassing forms of organization of public affairs or harmonization of relations and policies in a wider area than the municipal one, according to some criterion, in this case these are the borders of administrative deconcentration, where, in addition to purely administrative ones, other elements of connection at a wider level than the municipal one have a certain significance that can be used.

to replace a higher level of local self-government, or to establish quasi-authorities at a broader level.[5]

4. Regional Units of State Administration and Coordination of Relations

In all countries (except those consisting of only a few settlements, so-called city-states), there are regional units or authorities of state administration, i.e., some form of deconcentration. However, the role and number of regional authorities are not the same everywhere (e.g., single-tier or dual-tier systems). Additionally, the position of local self-government determines the role of regional units or authorities. In some countries (e.g., former socialist states), local self-government units are practically part of state administration authorities, with no clear distinction of tasks, often merely implementing decisions of central state authorities. In countries where such distinctions exist, self-government units, alongside their own competences, also perform some state tasks, over which they hold a significant degree of autonomy, with minimal (e.g., the Netherlands, Denmark, Germany, Czech Republic, etc.) or broader oversight powers of state authorities. In contrast, for regional authorities or units, hierarchical relations are complete (see Pusić, 2002, p. 83).

The establishment of regional authorities or units today is more commonly based on the principle of specialization, one per each administrative area, but there are also examples of omnibus regional authorities for all (or most) tasks within a narrower territory (with internal differentiation), usually overlapping with higher levels of self-government. This was typical in large states, particularly in the past, before specialization and differentiation of administration became dominant. Although clearly separated, these units also possess oversight powers regarding the work of self-governing units. In France, a unitary, decentralized state (Art. 1 of the Constitution), with three levels of self-government (Art. 72) and numerous institutional instruments linking them, and an imprecise and dynamic system of division of competences, there is a network of narrower administrative units – 342 districts (*Arrondissements*) and over 4,000 cantons (double tier). They act as centers of regional authorities

[5] In this context, one can cite the example of Portugal, which has a single-tier local government and strong resistance to political regionalization, and in which regional development and coordination councils have been established as forms of administrative regionalization, in which local governments participate. They represent a successful example of meeting regional needs and accessing EU funds (Ivanišević, 2009, p. 681).

state administration, but they also help departments in supervising communes. The function of the prefect before the 1982 reform included comprehensive control over decentralized units, and then was reduced to coordination and control of legality (Vučetić & Janićijević, 2006, p. 103.). Regional units formed according to the principle of specialization are often united at a wider territorial level by certain "omnibus" bodies, with the function of supervision, coordination, including hierarchical powers towards these units. In Serbia, regional units are formed according to the principle of specialization, with the head and the administrative district council as forms of unification, but without hierarchical powers.

The unitary nature of state administration, whose tasks are defined by the Law on State Administration (2005, Articles 12–21), implies that such tasks are performed throughout Serbia by republic-level administration bodies. This concept, however, is somewhat relativized. Namely, tasks of different levels of government are organizationally and functionally separated (Article 12 of the Constitution), but decentralized units may also perform delegated tasks of state administration (Lončar, 2014, p. 266), leading to some overlap. Still, constitutional provisions suggest that delegated competencies are an exception, and they are subject to a different legal regime than original competencies, even though performed by the same authorities. The difference pertains to organization, oversight, financing, inter-municipal cooperation, protection, etc. The purpose of delegation is defined in the Constitution as being "in the interest of more efficient and rational exercise of rights and obligations of citizens and satisfaction of their needs of immediate concern for their lives and work…" (Article 137). Most administrative tasks are performed by state authorities, with internal organization and deconcentration – *via regional units* regulated by laws, government decrees, and internal rulebooks.

If deconcentration is considered as a way of mitigating centralization, it should be functionally meaningful. The Law on State Administration (2005), lists the following administrative tasks: participation in shaping government policy, monitoring conditions, implementing laws, other regulations and general acts, inspection oversight, supervising public services, development tasks, and other professional tasks. Some of these are suitable for deconcentration by their nature, while others are not meaningful in this context (e.g., participating in policy-making, certain development tasks, regulation drafting, etc.). A state authority that decides to perform one or more administrative tasks in an administrative district establishes its regional unit through an act on internal organization and job classification (Article 38, para. 3). Internal subunits can also be formed within them. These *are parts* of state authorities, subject to

central leadership, which implies full hierarchical authority. In this regard, in addition to the right to determine internal organization and job classification, the head of the state authority holds the right to issue directives that define how employees operate and significant oversight and disciplinary powers.

Only certain tasks may be performed via regional units. The Law (Article 38) provides that in an administrative district, state administration authorities may, by their own decision, perform one or more tasks of state administration: "to decide administrative matters in the first instance; to rule on appeals when public authority holders have decided in the first instance; to supervise the work of public authority holders and to conduct inspection oversight." In this context, the question arises: is the legally limited scope of tasks that can be performed in regional units uniformly applicable to all authorities, and is it the most appropriate?

Administrative tasks are interconnected and conditional, they complement one another, and together, they give meaning to the function of public administration. By deciding on administrative matters, conducting inspections or other forms of oversight, and overseeing public services, authorities may also monitor conditions, which provides the basis for participating in policy-making. All of this is closely related to development tasks, which are mostly professional, and the execution of all these functions is most closely linked with internal oversight. The integration of regional and other organizational units within republic-level authorities, as centralized, hierarchical structures, ensures that various tasks are combined into a unified whole. Therefore, the performance of certain tasks through regional units, with appropriate internal organization and leadership, can improve the quality, effectiveness, or efficiency of task execution.

Material legislation defines administrative tasks in different fields, and the diversity of those fields entails a range of performance methods, including determining regional functions. Administrative tasks differ across fields, in complexity, procedures, and content; they consist of numerous interrelated operations, jobs, positions, organizational forms, and connections. Hence, the legal framework allowing deconcentration, which is implemented based on Government approval, should be flexible. If a ministry needs to perform some of its tasks at least partially through a regional unit, the law should generally provide for that possibility. This would strengthen the role of administrative districts, make certain tasks more effective, bring government closer to citizens, and allow internal organization to be aligned with actual needs in specific fields. Currently, regional units in some ministries already perform various tasks, including condition monitoring, professional duties,

particularly within oversight (e.g., education, construction, civil protection, general administration, social protection, environment, etc.).[6] Therefore, monitoring the situation, keeping records (which are kept for narrower areas, e.g. records kept by school administrations, etc.), issuing documents, taking care of public services (regional units of public services or school, health, cultural institutions), professional tasks ("collect and study data from their scope of work, prepare analyses, reports, information and materials and perform professional tasks that contribute to the development of the areas within their scope of work"), could be performed in district units. Also, instead of listing the possible ones, the legal norm could specify the tasks that cannot be performed in regional units (participation in policy-making, regulations,

[6] Within the *Ministry of Education*, school administrations function as regional units. In a school administration, the following tasks are performed: professional-pedagogical supervision of institutions; external evaluation of the quality of work in institutions; management of the lists of employees in educational institutions who are entitled to reassignment within the school administration; coordination of professional development; support for developmental planning, self-evaluation, development of preschool, school, and educational programs, and ensuring the quality of education; participation in the preparation of the development plan for education in its area and monitoring its implementation; ensuring that institutions maintain a database on education within the integrated education information system; cooperation with local self-government regarding the provision of budget funds for the professional development of employees in institutions; expert processing of cases and complaints related to the performance of professional-pedagogical supervision, and other tasks in accordance with the law. In the Department, sections or groups for sanitary supervision, as regional units of the *Ministry of Health*, the following tasks are performed: internal supervision of public authority holders in the area of sanitary oversight; drafting of reports on inspections of the work of sanitary inspectors within the Department, and based on the findings, proposing appropriate measures to the minister; participation in the preparation of expert foundations for drafting regulations in the areas under sanitary supervision; sanitary and health inspection in areas under sanitary oversight, including imposition of administrative measures and other actions in accordance with the law; issuing opinions on planning documents; issuing opinions on sanitary conditions in procedures for issuing urban-planning and technical requirements in construction processes for facilities under sanitary supervision; deciding administrative matters at the first instance, and other related tasks. Harbor master's offices are regional units of the *Ministry of Construction, Transport, and Infrastructure*, performing administrative, technical, and other professional tasks to ensure navigation safety, including: inbound and outbound checks at river border crossings; monitoring the movement and stay of vessels; initiating amendments to navigation regulations; undertaking administrative and other measures; issuing nautical requirements and nautical approvals; cooperating with organizations in the field of water transport; managing vessel traffic; issuing vessel documents and logbooks, as well as personal and other documents for crew members; performing technical and other professional tasks in the area of navigation; determining the seaworthiness of boats and floating structures; collecting statistical data on water transport; issuing decisions on vessel registration, maintaining vessel registries and records on vessels, crews, navigation, and the condition of waterways and navigation safety facilities; implementing wartime navigation regimes and taking measures in emergency situations.

unified records, certain development tasks). The tasks that are performed in regional units could be defined more precisely by decree and by-laws, according to the characteristics of individual administrative areas, the needs of certain parts of the territory, the content of certain tasks (e.g. monitoring the situation), etc. The law should also provide for the possibility that local self-government units can contact regional units to obtain an opinion or expert assistance in connection with the performance of the entrusted task, because regional units monitor the situation, carry out supervision, etc., as provided for in the Law on Local Self-Government (2007, Art. 80). The regional unit would be obliged to provide expert assistance in matters within its scope, thereby ensuring the preventive and advisory function of the district.

In accordance with the nature of the administrative district, as a regional center of state administration, the role of the district head can be defined as coordinating, declaratively supervisory, but non-decision making. However, it would be possible to add certain initiative and supervisory powers to it. Thus, he could initiate the adoption of directives or instructions, participate (through initiative or mandatory opinion-giving) in the procedure for taking over delegated competencies (Art. 56 of the Act on State Administration), propose the joint performance of entrusted competencies by several municipalities (Art. 75 of the Act), etc. Due to the proximity of the entities performing entrusted work, the mayor of the administrative district may have more direct and complete knowledge regarding their performance, as well as the personnel and other resources of the municipalities. Namely, the head of the administrative district monitors the work of regional units, the implementation of plans, instructions, etc., he therefore possesses appropriate information regarding the performance of delegated competencies, but without the ability to act in this regard, therefore, supplementing his role with the ability to propose the taking of appropriate measures, to present the issue to the district council, initiate proceedings, etc., is in the function of fulfilling his role. This does not interfere with the powers of regional units in the performance of supervision, but rather their more effective coordination is carried out, and his declarative role of supervision gains some meaning.

Some of the modern local functions, such as local development planning, environmental protection, healthcare, protection against natural disasters, the establishment of cultural institutions, tourism development, etc., often exceed the material, personnel, and organizational capacities of a large number of municipalities. In comparative law, it is not uncommon that, during the planning of the local budget, the adoption of planning and development acts, for major investment projects, or for activities of particular importance to several local

communities, more formalized cooperation is established and certain relations regulated between municipalities and regional units of state authorities (often also with development bodies, economic organizations, etc.) – such as regular consultations, deadlines for undertaking specific actions, information sharing, harmonization of plans, projects, etc. The level of formalization can be even greater, in the form of multilateral cooperation agreements, joint bodies, regular consultations, public debates, and even the establishment of joint services (in the areas of education, healthcare, culture, sports, information, etc.). The management of certain public affairs requires the involvement of multiple levels of government, and the undertaking of a set of measures that exceed the competences of each one individually. These affairs require complex regulation, a larger number of involved actors, greater financial resources, a complex system of control, i.e., institutional cooperation between local self-government, regional administration, public services (e.g., consortia in Spain). It is difficult to achieve public interest if the actors to whom the respective policy or regulation applies are not consulted already in the initial phase of its formulation. Cooperation in the final phase, when it is practically impossible to influence changes to the basic framework of an already established regulatory system or where the consultative function is merely declarative, does not contribute to achieving public interest and the goals of adopting such strategies or regulations (Jerinić & Pavlović-Kržanić, 2010, p. 11).

Institutional cooperation of non-central units can be realized through the council of the administrative district. The primary role of this body is to harmonize relations between the regional units of the authorities and the municipalities and cities from its area, and to make proposals for improving their work. It cannot include subordination, decision-making, or subsidiarity, but through the possibility of initiative, coordination, and exchange of information, it can provide an institutional mechanism for dialogue, harmonization of relations and common interests, and thus influence the effectiveness of tasks that require the participation of various units and levels. In this regard, the role of the administrative district council could include the following: encouraging and guiding inter-municipal cooperation in delegated competencies,[7] initiating the implementation of internal supervision, proposing the adoption of planning documents, drafting analyses, giving opinions on planning

[7] This procedure is regulated by the Law (Art. 75), with the wording and manner of joint execution of the entrusted tasks being regulated by a Government decree. In this regard, the opinion of the administrative district council could also be taken into account, previously or subsequently, as a body called upon to take a position. In addition, cooperation would acquire a planned and directed character, primarily (not always and exclusively) within the administrative district.

documents and regulations of importance to the administrative district area (waste management, environmental protection, emergency situations, etc.), considering issues related to the staffing structure for performing delegated or regional unit's competencies,[8] proposing its improvement, and even expressing an opinion on the manner of performing delegated competencies at the request of a municipality. For example, in case of doubt regarding the ability of a particular municipality to perform entrusted tasks in a timely or lawful manner, the issue could be discussed at the council, and the intervention of a state body could be requested. The administrative district council could also establish coordination bodies for guiding tasks within the competences of the regional unit and/or multiple local self-government units – for example, on issues of natural disasters, environmental protection, communal services, etc. – where different levels possess certain competences, and where there is a need for coordination and harmonization, especially at the operational level, which can be further regulated by a government decree.

5. Administrative Supervision and Administrative Districts

The Law on State Administration (2005) stipulates that supervisory tasks may be performed within regional units, including inspection supervision, which is regulated by a separate law. Tomić (2016, pp. 163–164) speaks of three types of administrative supervision in our regulations: 1) work supervision; 2) inspection (regulated by a separate law); 3) internal administrative supervision regulated by the Law on General Administrative Procedure (2016), (legal remedies) and other laws. State administration bodies in the district can carry out all types of administrative supervision. Supervision of operations encompasses general and specific oversight powers over all entities entrusted with competencies, as well as certain supervisory matters related to the performance of original competences by decentralized units. The relationship between state authorities and decentralized units in terms of preventive and advisory actions by the state administration – repeatedly emphasized in the planning documents mentioned – must also be considered in relation to the provisions of the Law on Local Self-Government

[8] The consideration of the personnel structure and the provision of recommendations regarding it should be viewed in the context of the provisions of the Law on Civil Servants and the Law on Employees in APs and Local Government Units, where the possibilities of taking over or seconding officials – rational use of the personnel structure of different levels, can be more effectively realized with the participation of the administrative district council, which would monitor, consider and make recommendations on this issue at the district level.

(2007), regarding the submission of initiatives, proposals, and consultations (Articles 78–80). These issues are not precisely regulated, and there is a need to define deadlines for responses, approvals, and opinions, at least in general terms, allowing sectoral laws to further regulate them based on the specific requirements of tasks in their respective fields.

The issue of supervision is quite comprehensively regulated in the Law on State Administration (2005, Articles 46–57). The scope of oversight powers corresponds to the nature of delegated tasks, for which the Republic retains responsibility. The exercise of supervision is highlighted in programming documents: "The administrative district can and should be one of the key mechanisms for developing the national system of supervision and inspection, which will act solely *for the purpose of ensuring legality and provide positive direction to lower levels of government*" and "strengthening the coordination role of administrative districts and their supervisory function over the execution of tasks by local self-government, especially their *preventive and advisory functions* in areas of supervision conducted by state authorities." However, it is important to emphasize that administrative district bodies cannot themselves hold supervisory authority, but they can participate in the supervision system and in "positive guidance", and make use of the existing legal possibility that certain supervisory tasks may be carried out in regional units, through specific authorizations in sectoral laws, which could be expanded. Regarding the role of the regional unit within the supervision system, the system of internal relationships within state administration bodies is also relevant, including the powers of managers (e.g., directives), as well as instructions as a general supervisory tool, which guide the organization of work and procedures for employees and public authority holders in performing delegated tasks. However, such instructions may not define the manner of handling or decision-making in individual administrative matters and cases (Article 48). It is considered inadvisable to introduce new mechanisms or to precisely define existing ones through this law as a systemic act, which lacks field-specific solutions and cannot emphasize a special purpose of general legal institutions – that would be better handled through sectoral legislation.

Regarding oversight of regulations adopted by holders of public authority, it is necessary to consider specifying certain deadlines from the Law on State Administration (2005, Article 57): "A holder of public authority is obliged to obtain an opinion from the competent ministry on the constitutionality and legality of a regulation before its publication. The ministry shall then provide a reasoned opinion on how the regulation may be aligned with the Constitution, law, or other general acts of the National Assembly or the Government. If

the public authority does not act upon the opinion, the ministry is obliged to propose to the Government to annul or repeal that regulation if it is not in conformity with the acts of the National Assembly or Government, or if it is not in accordance with the Constitution or law, to propose that the Government suspend its application and initiate proceedings for a review of its constitutionality or legality."

Given the significance of such opinions by ministries and the need highlighted in the planning documents to ensure expert support and act preventively, it is necessary to consider defining a deadline within which the ministry must provide a reasoned proposal for aligning the regulation with higher-level legal acts. The length of such a deadline requires consultation with examples of good practice in state administration. Thus, the proposal for such a deadline can only be interpreted as indicative. That deadline could also be of instructive character, serving to ensure procedural discipline.

6. Conclusions and Recommendations on Improving the Legal Framework

The expansion of the role of the administrative district can be observed through 1) the expansion of the role of regional units within the district, and 2) the expansion of the role of the District Head and the District Council. Any legislative intervention concerning these matters must take into account the nature of the administrative district and its bodies – that it is not a level of government, and that the role of its bodies is limited to coordination, harmonization, cooperation, initiative, and participation, which may be part of the procedure for adopting certain acts (planning, regulatory, or technical) or oversight. These roles cannot substitute for the authority to adopt acts, but the level of supervisory powers may be strengthened, harmonization efforts specified, and the obligation to provide professional assistance in the area of delegated tasks more precisely defined. Moreover, the need for dislocation of tasks is not uniform across different authorities, and the legal limitation on which tasks may be performed in regional units can be restrictive, potentially having a counterproductive effect in certain administrative areas or tasks. Therefore, the Law on State Administration should be formulated more flexibly in this regard. After all, each state administration authority defines its internal structure and task deconcentration with the approval of the Government. This procedure already includes sufficient safeguards to prevent misuse of these provisions. In addition, the sectoral laws may further expand the role of the administrative district.

The relationship between state administration bodies and local self-government bodies, beyond supervisory powers, is set out in principle, and as such is vague and even ineffective. It is mainly left to be regulated by sectoral laws or is based on limited examples of good practice. It would also be appropriate to prescribe a general deadline for all procedures in which the relationship between two-level bodies is manifested, which would have subsidiary application.

Golić Darko
Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, Srbija

ULOGA UPRAVNIH OKRUGA U UPRAVNOM SISTEMU SRBIJE

APSTRAKT: U radu se analizira uloga upravnih okruga i područnih jednica organa državne uprave, te potrebe i mogućnosti njihove reforme. Necentralni aspekt javne uprave i sam predstavlja složenu celinu sa više različitih elemenata, međusobnih odnosa i potreba. S tim u vezi, analiziraju se mogućnosti i načini „*jačanja upravnih okruga*“, te „*unapređenja vertikalnog i horizontalnog nadzora u obavljanju izvornih i poverenih poslova*“ necentralnog nivoa*,* kako je to određeno važećim planskim dokumentima. Okosnicu ovog razmatranja čine pozitivnopravna rešenja, te strateški i planski dokumenti u Srbiji, uz odgovarajuće komparativne osvrte. Osnovna istraživačka dilema se odnosi na ograničene mogućnosti da se unapredi vršenje poslova državne uprave putem ili unutar upravnih okruga. Ona proističe iz karaktera necentralnog aspekta javne uprave, kao složenog podsistema, sa dve komponente – lokalnom samoupravom sa svojim izvornim poslovima (decentralizovani aspekt), te lokalnom samoupravom sa poverenim poslovima i područnim jedinicama organa državne uprave (manje ili više centralizovani aspekt), u pogledu kojih postoje odgovarajuće veze putem upravnog okruga.

Ključne reči: *upravni okrug, dekoncentracija, načelnik i savet upravnog okruga.*

References

1. Borković, I. (1981). *Upravno pravo* [*Administrative Law*]. Zagreb: Informator
2. Golić, D. (2014). Normativni okviri regionalizacije javnih poslova u Srbiji [Normative frameworks for the regionalization of public affairs in Serbia]. In: Davitkovski, B. (ured.)*, Godišnik na Pravniot fakultet „Justinijan Prvi“ vo Skopje* [*Yearbook of the Faculty of Law "Justinian the First" in Skopje*] (pp. 148–150). Skopje: Faculty of Law "Justinian the First"
3. Ivanišević, S. (2009). Stupnjevanje lokalnih samoupravnih jedinica [Graduation local self-governing unit]. *Hrvatska javna uprava*, *9*(3), pp. 669–722
4. Jerinić, J., & Pavlović Križanić, T. (2010). *Horizontalna i vertikalna koordinacija u postupku donošenja odluka od značaja za lokalnu samoupravu u Srbiji* [*Horizontal and vertical coordination in the decision-making process of importance for local self-government in Serbia*]. Beograd: PALGO centar
5. Kostić, L. (2000). *Sabrana dela – Prvi tom: Administrativno pravo Kraljevine Jugoslavije* [*Collected Works – Volume One: Administrative Law of the Kingdom of Yugoslavia*]. Beograd: ZIPS SRS
6. Lapčević, M., & Rapajić, M. (2023). On local self-government and its constitutional and legal position in Serbia. *Pravo – teorija i praksa, 40*(4), pp. 112–137. https://doi.org/10.5937/ptp2304112L
7. Lončar, Z. (2014). Povereni poslovi državne uprave u oblasti zaštite životne sredine [Entrusted state administration affairs in the field of environmental protection]. *Zbornik radova Pravnog fakulteta u Novom Sadu*, *48*(3), pp. 265–278
8. Marković, R. (2015). *Ustavno pravo* [*Constitutional Law*]. Beograd : Pravni fakultet Univerziteta, Centar za izdavaštvo i informisanje; Dosije studio
9. Milkov, D. (2009). *Upravno pravo – uvodna i organizaciona pitanja* [*Administrative law – introductory and organizational issues*]. Novi Sad: Pravni fakultet u Novom Sadu
10. Petrović, M. (2006). *Nauka o upravljanju kao pretpostavka upravne politike – opšti deo* [*Management Science as a prerequisite for administrative policy – general part*]. Niš: Pravni fakultet – Centar za publikacije

11. Program reforme sistema lokalne samouprave Republike Srbije (2021–2025) [Local Self-Government System Reform Program of the Republic of Serbia (2021–2025)]. Downloaded 2025, January 25 from https://lsg-monitoring.mduls.gov.rs/
12. Pusić, E. (2002). *Nauka o upravi* [*Science of management*]. Zagreb: Školska knjiga
13. Strategija reforme javne uprave u Republici Srbiji za period od 2021. do 2030. godine [Public Administration Reform Strategy in the Republic of Serbia for the period 2021-2030]. *Službeni glasnik RS*, br. 42/21 i 9/22
14. Tomić, Z. (2016). *Opšte upravno pravo* [*General Administrative Law*]. Beograd: Pravni fakultet Univerziteta
15. Uredba o upravnim okruzima [Decree on Administrative Districts]. *Službeni glasnik RS*, br. 15/06
16. Vlatković, M., & Golić, D. (2021). *Pravo lokalne samouprave* [*Local Self-Government Law*]. Novi Sad: Pravni fakultet za privredu i pravosuđe
17. Vučetić, D. (2012). *Decentralizacija u kontinentalnim pravnim sistemima. Doktorska disertacija* [*Decentralization in continental legal systems*]. Niš: Pravni fakultet Univerziteta u Nišu
18. Vučetić, D., & Janićijević, D. (2006). *Decentralizacija kao polazište daljeg razvoja Srbije* [*Decentralization as starting point for the further development of Serbia*]. Niš: Centar za razvoj građanskog društva „Protecta"
19. Zakon o državnoj upravi [Law on State Administration]. *Službeni glasnik RS*, br. 79/05, 101/07, 95/10, 99/14, 47/18 i 30/18 – dr. zakon
20. Zakon o lokalnoj samoupravi [Law on Local Self-Government]. *Službeni glasnik RS*, br. 129/07, 83/14 – dr. zakon, 101/16 – dr. zakon, 47/18 i 111/21 – dr. zakon
21. Zakon o opštem upravnom postupku [Law on General Administrative Procedure]. *Službeni glasnik RS*, br. 18/16, 95/18 - autentično tumačenje i 2/23 - odluka US

Vasilkov Zorančo[*]
https://orcid.org/0000-0001-8282-2777
Ristić Vladimir[**]
https://orcid.org/0000-0002-2450-3417

UDK: 004.8:341.222
Original scientific paper
DOI: 10.5937/ptp2502036V
Received on: March 11, 2025
Approved for publication on:
April 29, 2025
Pages: 36–48

ARTIFICIAL INTELLIGENCE AND EU INTEGRATED BORDER MANAGEMENT

ABSTRACT: The future development of artificial intelligence and the expansion of its application across many areas of social life represent a global phenomenon. The normative regulation of artificial intelligence development within international organizations has become a dynamic process throughout 2024. Considering both the potential benefits of artificial intelligence for humanity and the possible devastating effects on human rights, the EU—as a leading international regulatory entity—has established a legal framework for the use of artificial intelligence in nearly all areas of public governance, including migration, asylum, and the management of its external borders.

This paper examines the emergence, connection, significance, and integration of artificial intelligence in border control, as well as the relevance of EU legal norms for its current and future application within the model of integrated management of the EU's external borders. A key focus of the research is the implications of artificial intelligence use on the fundamental rights of vulnerable groups, alongside the role of Frontex in researching the application of specific artificial intelligence systems in border and migration management.

[*] PhD, Assistant Professor, University MB, Faculty of Business and Law, Belgrade, e-mail: vasilkovzoranco@yahoo.com
[**] PhD student, Master of Security Management, Directorate for Police Training of the Ministry of Interior of the Republic of Serbia, Belgrade, e-mail: ristic.vladimir11@gmail.com

Keywords: *artificial intelligence, integrated border management, legal framework, Frontex.*

1. Introduction

Building an EU legal framework for the use of high technologies, in particular artificial intelligence (AI) for the benefit of every citizen, has been a priority for EU institutions for almost 10 years. Taking into account the potential of AI and the overall benefit for humanity, as well as the possible devastating effect on human rights, the EU, as a leading international regulatory entity, has managed to establish a legal framework for the use of AI in almost all areas of social life, including the areas of migration, asylum and control, i.e. management of external borders. In the paper, the authors consider the conditionality, connectivity and potential impact of AI systems on external border management, more specifically they explore the approach of the EU and its supranational border agencies in the possible use of AI systems within the framework of integrated border management (IBM). The starting point is to establish a concept or model of IBM and a legal basis for the potential application of modern technologies and AI in IBM with an emphasis on the specific tasks of the European Border and Coast Guard (EBCG), which could be significantly impacted by AI systems. The authors also point to the efforts of human rights advocates during the negotiations on the Act (Regulation) on Artificial Intelligence (AIA) in order to mitigate the risks of using high-risk AI systems in the context of border and migration management. Finally, the paper presents Frontex's research activities on the application of various artificial intelligence systems that would enable more efficient control and management of the Union's external borders.

2. The connection between research on the use of new technologies and AI and the IBM Model

An in-depth analysis of the relationship between artificial intelligence and IBM in the function of EU border control requires a brief definition and presentation of the concept of IBM. The term "Integrated Border Management" means national and international coordination and cooperation between all relevant authorities and agencies involved in border security and trade facilitation, with the aim of establishing an effective, efficient and coordinated management of the EU's external borders (European Commission, 2024). Coordination includes measures between institutions, hierarchically

and horizontally placed and integrated at the European and national level (Ristić, 2022). The goal is to maintain open but well-controlled and secure borders. The IBM model has been developing in the EU since 1999, after the integration of the Schengen Agreements (the Schengen Agreement and the Convention on its Implementation) into the EU legal framework (Božovic & Vasilkov, 2020, p. 108). As an integral part related to the control of migration and external borders, this model appears in the conclusions of the European Council from Tampere from 1999, also known as the Tampere Program for the Area of Freedom, Security and Justice (European Council, 1999, points 24–25). Even then, the European Council emphasized the necessity of the exchange of technical assistance and the transfer of technologies between member states as a key issue for successful border control. The management of the Union's external borders is directly mentioned and linked to the functioning and future expansion of the Schengen area in the conclusions of the European Council from Leken in 2001 (European Council, 2001, point 42). Based on these conclusions of the European Council, and the attempts of the European Commission to define IBM from a supranational level, the Council of the EU formally established a harmonized system for IBM in 2006 (Council of the EU, 2006). It can be said that in the very conception of the IBM model for improving the work and carrying out the tasks of the border services, technical technological assistance, technology transfer and research is incorporated, which is later unified by the use of AI in the management of the external borders of the Union.

The uncertainty regarding the legal basis and place of the IBM in the legal order of the Union was finally removed with the adoption of the Treaty of Lisbon. Namely, the Treaty on the Functioning of the European Union (TFEU) introduces a provision on the "gradual establishment of integrated management of external borders" into the Union's primary law. (Treaty of Lisbon, 2016, Article 77 1(c) TFEU). This provision was used as the legal basis for the establishment of the European Border and Coast Guard and the expansion of the mandate of its Agency (established in 2004) known as Frontex. With the establishment of the European Border and Coast Guard and its transformation in 2016, and especially in 2019, the IBM model became part of the Agency's mandate, which includes powers to research the application of state-of-the-art technologies to perform border control tasks (Regulation on EBCG, 2019/1896, Article 3). Namely, as a result, "evolutionary" provisions are included in the IBM model that foresee, allow and encourage the research and application of AI, thus enabling Frontex, in cooperation with private high-tech companies, to intensively research and experiment with AI systems

as a tool for effective control of external borders. Two essential elements of IBM support the introduction and implementation of the AI system: the use of state-of-the-art technology, including large-scale information systems (Regulation on EBCG, 2019/189, Article 3, paragraph J), and research and innovation (Regulation on EBCG, 2019/1896, Article 3, point 2).

Significant for a deeper understanding of the application of AI are also the activities of the European Commission from 2023 to establish a multi-year strategic policy for European integrated border management (Strategy of the European Commission on IBM), in which this institution provides explanations and recommendations for the use of AI within the IBM (COM/2023/146 final). This document places IBM in a global context, placing it as a high political priority, i.e. formalizing what has long been a politically driven priority aimed at controlling borders and migratory flows. In the Annex to the Strategy, specific guidelines are given for the implementation of each of the fifteen established elements of IBM, offering specific directions for its future development. For example, in connection with the use of state-of-the-art technology, including large information systems (element 10), the Strategy envisages support for advanced, mobile and interoperable European technical systems and solutions that are compatible with large EU information systems. Therefore, the use of modern technologies, especially AI systems, is recommended to improve European surveillance and response capabilities at the Union's external borders, using satellite technology to create a comprehensive overview of the situation within the specialized border surveillance system, which as a separate system known as Eurosur since 2019. functions within Frontex (Regulation on EBCG, 2019/1896, Part 3). For more effective surveillance, it is advised to expand the control capacities of integrated, interoperable and adaptable technical systems (both stationary and mobile) that are based on AI systems and are used at sea and land borders. This extension should cover the technical solutions and operational procedures used in the various operational centres (such as national coordination centres, rescue coordination centres and local coordination centres) and mobile units (Guidelines 4–6, Annexes 1 and 2, COM/ 2023/146 final, p. 21).

Regarding research and innovation within IBM, the policy priorities emphasize the crucial link between all research projects related to border management and security, emphasizing the need for synergy between research projects within Horizon Europe and other EU funding programmes. To achieve these priorities, specific guidelines are recommended to enhance research and innovation in border management operations, with the aim of making them more interoperable, cost-effective and sustainable. Member States'

border authorities, together with Frontex and EU-LISA, are recommended to actively monitor research and innovation in order to improve IBM by introducing and using new innovative solutions. More specifically, the focus is on harnessing the potential of AI, promoting the exchange of solutions and best practices, while acknowledging the sensitivity, complexity and potentially high risks associated with AI-based solutions. Ethical principles, adaptability and reliability of AI tools in the protection of human rights must be a priority in border management research and innovation. This means that the AI systems used within IBM should be subject to all necessary safeguards, control mechanisms and protection levels provided by the EU Regulation on AI (Guidelines 1 and 9, Annexes 1 and 2, COM/2023/146 final, p. 29).

The aforementioned Regulation of the European Parliament and the Council on the establishment of harmonized rules on artificial intelligence establishes a broad legal basis for the future development and use of artificial intelligence systems in the EU and member states (in EU literature and documents, the name Artificial Intelligence Act – AIA is most often used, which will be the case below). AIA as an act of secondary legislation, starts and introduces into the legal framework the assessment of the risk of damage that AI systems can represent to fundamental rights, defining the application of individual AI systems in various areas as high-risk (AIA Regulation (EU) 2024/1689). For "migration, asylum and management of state border control" which includes both control and management of the Union's external borders, high-risk AI systems that can be used are listed, i.e. when and for what purposes their use is allowed (AIA Regulation (EU) 2024/1689, Annex 3). Such AI systems are subject to higher standards for approval, oversight and, in particular, accountability for their implementation established for manufacturers, operators and end users. In this sense, it is necessary to look at and examine the relevance and connection between AI and IBM.

3. Relevance and connection of AI with IBM

When examining the relevance or connection of AI and IBM, we start from the assessment of potential risks and dangers of using high-risk AI systems and the possibility of causing disproportionate damage to human rights during their application. It is evident that a high degree of danger arises from AI systems that use biometrics, specifically remote biometric identification and categorization (AIA Regulation (EU) 2024/1689, Annex 3 point 1), as well as those that include special techniques for law enforcement, i.e. prosecution and policing (AIA Regulation (EU) 2024/1689, Annex 3, point 6), most of which

also apply to border control and surveillance. In addition, there is a specific categorization of high-risk AI systems that would be used for migration control, asylum and border management purposes. Their introduction and use is aimed at screening techniques for migrants at external borders or within the Schengen area (such as polygraphs and similar tools), performing risk assessments (including security assessments related to irregular migrants or health risk assessments for individuals entering or intending to enter the territory of member states), processing requests for asylum, visas or residence permits and techniques for detecting, recognizing or identifying individuals during border surveillance (AIA Regulation (EU) 2024/1689, Annex 3, point 7).

If we connect these provisions of the AIA and the authorizations for the application of specific AI systems to the tasks or components of the IBM defined in Article 3 of the Regulation on EBCG, their direct applicability is obvious in: 1) state border surveillance, which includes measures to facilitate legal border crossing and, as appropriate, preventing and detecting cross-border crime at external borders, such as migrant smuggling, human trafficking and terrorism. This includes mechanisms and procedures for the identification of vulnerable individuals, unaccompanied minors and those who need or seek international protection, with the provision of information and referral to established procedures; 2) search and rescue operations, 3) risk analysis for internal security and assessment of threats that could affect the work of competent authorities or the security of external borders; 4) exchange of information and cooperation between member states; 5) inter-institutional cooperation at the national and supranational level; 6) cooperation with third countries; 7) implementation of technical and operational measures within the Schengen area with the aim of improving border surveillance, suppression of illegal immigration and the fight against cross-border crime; and especially 8) protection of basic rights of migrants, seekers of international protection (asylum), especially protection of extremely sensitive and vulnerable groups such as unaccompanied minor migrants, women with children and divided families.

Within the framework of relevance, it is necessary to analyse certain aspects of the protection of human rights. High-risk AI systems used or planned for use in border, migration and asylum management often significantly affect the vulnerable groups of people who rely on the outcomes of legal, administrative and discretionary procedures of competent public authorities of member states. This is precisely where the substantive legal deficiencies of the AIA are reflected, which does not classify as high-risk all AI systems that

are inherently discriminatory, and are used to assess threats from migrants and asylum seekers to public order and security of the member states of the Union itself (Vasilkov, 2024, p. 3). That is why it is necessary that AI systems in this area, before use, be subject to a higher level of accuracy, testing of non-discriminatory nature and transparency, in order to ensure the protection of human rights. Such an approach in this particular case would mean that the implementation of the AI system should be conditioned by adequate protection of migrants' rights to freedom of movement, privacy, protection of personal data and the right to good governance (Dumbrava, 2021, p. 28).

Some of these issues were in the public spotlight before the adoption of the AIA itself, when non-governmental organizations and human rights defenders demanded a ban on the use of the AI system, which dramatically threatens basic rights. It is highly invasive AI, built on biased or unscientific assumptions, and would be used for biometric categorization of people, facial recognition and identity verification, emotion and lie detection during interrogation as well as remote biometric identification and mass border surveillance. The prohibited practice of using VI should have included its use for illegal rejection of irregular migrants by border services and profiling of individuals in movement (EDRI, 2023). If we add to this surveillance via the Internet of Things (IoT) and the collection or extraction of personal data from smart devices such as mobile phones, laptops or any other device that can connect to the Internet in migrant reception centres (Domazet, Marković & Skakavac, 2024), then the wider picture of surveillance via the AI system is frightening. Such discrimination, surveillance and total control would have unfathomable consequences, exposing migrants and asylum seekers to additional difficulties and even greater risks for their already endangered basic rights (Jones, Lanneau & Maccanico, 2023, p. 27). Some of these proposals were included in the amendments of the European Parliament and helped to introduce changes and improve the original text of the Commission, primarily by introducing in the AIA the right to submit a complaint to the competent authorities regarding the violation of fundamental rights. However, the final version of the AIA weakened this right by not prescribing the obligation of these authorities to respond to such complaints (Friedl & Gasiola, 2024, p. 3).

4. AI at IBM from Frontex's perspective

Will artificial intelligence systems really be used to combat migration and unwanted asylum seekers as the biggest threat to the EU? Will the capacities of AI and border officers lead to a symbiosis that will ensure greater security

of external borders, the Schengen area as an area without internal borders and the security of citizens, member states and the Union itself? It is unlikely that this will be the case, just as it is difficult to accept that migrants are the biggest threat to the EU. This will not prevent the new reality called mass surveillance and border control using AI systems whose expansion is yet to follow. The basic idea of the use of VI, which originates from various documents of the EU institutions in this field, is closely related to the efforts aimed at improving the current and future performance of the European Border and Coast Guard in implementing its mandate and carrying out the tasks arising from the IBM.

In this context, a study on the impact of AI systems on the Schengen acquis related to migration, IBM and EU security has already been carried out. In particular, an examination of the impact of the use of AI systems on part of the internal and external processes for the management of EU borders, migration and security was carried out, in relation to :1) Issuing visas for a short stay, 2) Issuing ETIAS travel permits, 3) Issuing documents for a longer stay or stay in the Schengen zone, 4) Granting international protection 5) SIS consultations and the involvement of the SIRENE bureau, 6) Border controls at external Schengen borders 7) Operational management of services in eu-LISA, 8) Process of creation and implementation of EU policy related to the Schengen area, and 9) Transversal processes and opportunities of interested parties (European Commission, 2020, p. 2). At the same time, special emphasis was placed on the analysis of the feasibility of developing forecasting and early warning tools based on AI technology that would be capable of predicting and assessing the direction and intensity of irregular migration flows to and within the EU in real time. Based on this, AI systems should be able to provide early warnings and forecasts both in the short term for the period of 1 to 4 weeks and in the medium term for the period of 1 to 3 months. The value of these tools should be the provision and distribution of reliable assessments to the European Commission and EU member states for successful migration management, i.e. planning and organization of common resources in border management. Monitoring objects on which all AI tools and systems should be applied are mixed migration flows to the EU and complex population movements that include refugees, asylum seekers, economic migrants, victims of human trafficking, smuggled migrants, unaccompanied minors, etc. (European Commission, 2021, p. 2). Furthermore, functions performed by AI systems in these areas include risk assessment and profiling, identity verification and fraud detection, behaviour or emotion recognition, speech recognition, mobile phone data extraction, electronic tracking and future mobility prediction. AI systems that perform these functions include

chatbots and intelligent agents, risk assessment tools, knowledge management tools, policy insight and analytics tools, and computer vision tools (European Commission, 2020, p. 56).

Frontex's involvement in these current researches and especially the future use of AI systems to carry out tasks related to border controls, is under the scrutiny of the public, especially human rights defenders, who have long pointed to the abuse of authorization and omissions in the work of Frontex. Border law enforcement by Frontex itself is often characterized as a systematic violation of the rights of illegal migrants (López, 2023, p. 2). The use of AI systems in the field of border control and migration, as well as the implementation of tasks within the framework of IBM, will definitely represent progress in preserving the physical and digital security of the "stronghold of the EU" (Vasilkov, 2023, p. 40) with a serious setback or a devastating reduction in the scope of guaranteed human rights of migrants and vulnerable categories of persons, which will further threaten and reduce the credibility of the Union in respect of its own values on which it was built.

5. Conclusion

AI as part of the incentive to use the most modern technologies and technological assistance in the management of external borders are areas connected since the time the built and elaborated IBM model entered the scene. Research into the use of the AI system for the protection of the EU's external borders and the support of the IBM remains a very sensitive issue even after the adoption of the AIA. AIA is a milestone, which nevertheless confirms that AI systems are not just technological tools for meeting border control standards. Analyzing the relevance of the legal framework, the enormous potential of using AI for the improvement of IBM is presented, but also an even greater potential and danger for endangering human rights. Threats to human rights in this area do not prevent the determination of member states, EU institutions, and especially Frontex in researching practical application in various domains of border controls as part of the overall strategy to control irregular migration and migration flows that the Union is facing or will face in the future.

In addition to the insistence on respect of human rights and basic freedoms in the EU, the use of the VI means the creation of new barriers for vulnerable categories, migrants and asylum seekers who do not have, and will hardly in the future with the VI, have sufficient guarantees that their rights will be respected. Namely, even without the use of the VI there were enough

difficulties and inconsistencies in the application of their rights at the external borders in contact with the border services of the member states and Frontex. Gradual and frequent reliance on VI systems, especially the use of biometrics, continuous mass monitoring of the external borders of the Union, as well as all the research currently being conducted, speak in favor of a greater degree of ensuring internal security through the implementation of IUG as an EU priority, without too much concern for human rights, i.e. the application of legal instruments and remedies for violated rights of vulnerable categories of persons.

Vasilkov Zorančo
Univerzitet „MB“, Poslovni i pravni fakultet, Beograd, Srbija

Ristić Vladimir
Uprava za policijsku obuku Ministarstva unutrašnjih poslova Republike Srbije, Beograd, Srbija

VEŠTAČKA INTELIGENCIJA I INTEGRISANO UPRAVLJANJE GRANICOM U EU

APSTRAKT: Budućnost razvoja veštačke inteligencije i širenje njene primene u mnogim oblastima društvenog života je globalni fenomen. Normativno uređenje razvoja veštačke inteligencije u međunarodnim organizacijama postaje dinamičan proces tokom 2024. godine. Uzimajući u obzir potencijal veštačke inteligencije i sveukupnu korist za čovečanstvo, kao i mogući razarajući efekat na ljudska prava, EU je kao vodeći međunarodni regulatorni entitet uspela da uspostavi pravni okvir za korišćenje veštačke inteligencije u gotovo svim oblastima javnog delovanja, uključujući oblast migracija, azila i kontrole, odnosno upravljanja njenim spoljnim granicama.

U ovom radu autori istražuju pojavu, povezanost, značaj i uključivanje veštačke inteligencije u kontrolu granica i relevantnost pravnih normi EU za njeno trenutno i buduće korišćenje u okviru modela integrisanog upravljanja spoljnim granicama EU. Nezaobilazan deo istraživanja su

implikacije primene veštačke inteligencije na osnovna prava ugroženih kategorija lica i uloga Fronteksa u istraživanju primene specifičnih sistema veštačke inteligencije u upravljanju granicama i migracijama.

Ključne reči: *veštačka inteligencija, integrisano upravljanje granicom, pravni okvir, Frontex.*

References

1. Artificial Intelligence Act – AIA. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828, OJ L, 2024/1689, 12/7/2024
2. Božović, M., & Vasilkov, Z. (2020). Integrisano upravljanje granicama u EU i njena primena u Republici Srbiji. [Integrated Border Management in the EU and its Implementation in the Republic of Serbia]. *Bezbednost*, *62*(3), pp. 105–123
3. European Commission (2023). Communication from the commission to the European Parliament and the Council establishing the multiannual strategic policy for European integrated border Management. COM (2023) 146 final.
4. Council of the European Union (2006). 2768th Council Meeting Justice and Home Affairs, Brussels. Downloaded 2024, November 16 from https://ec.europa.eu/commission/presscorner/detail/en/pres_06_341
5. Domazet, S., Marković, D., & Skakavac, T. (2024). Privacy under threat – The intersection of IoT and mass surveillance. *Pravo – teorija i praksa*, 41(3), pp. 109–124
6. Dumbrava, C. (2021). *Artificial intelligence at EU borders – Overview of applications and key issues*. European Parliamentary Research Service EPRS. Downloaded 2024, November 16, from https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf
7. EDRi (2023). EU Parliament calls for ban of public facial recognition, but leaves human rights gaps in final position on AI Act. Downloaded 2024, November 18 from https://edri.org/our-work/eu-parliament-plenary-ban-of-public-facial-recognition-human-rights-gaps-ai-act/

8. European Commission. European integrated border management. Downloaded 2024, November 15 from https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-asylum-and-migration-glossary/glossary/european-integrated-border-management_en
9. European Commission: Directorate-General for Migration and Home Affairs (2020). Opportunities and challenges for the use of artificial intelligence in border control, migration and security. Volume 1, Main report. Publications Office. Downloaded 2024, November 22 from https://data.europa.eu/doi/10.2837/923610
10. European Council. (1999). Presidency conclusions tampere European Council 15 and 16 october 1999. Downloaded 2024, November 21 from https://www.europarl.europa.eu/summits/tam_en.htm
11. European Council. (2001). Presidency conclusions European Council meeting in laeken 14 and 15 december 2001. Downloaded 2024, November 21 from https://www.consilium.europa.eu/media/20950/68827.pdf
12. Friedl, P., & Gasiola, G. G. (2024). *Examining the EU's Artificial Intelligence Act, VerfBlog,* 2024/2/07. DOI: 10.59704/789d6ad759d0a40b. Downloaded 2024, November 17 https://verfassungsblog.de/examining-the-eus-artificial-intelligence-act/
13. Frontex – European Border and Coast Guard Agency (2021). *Artificial Intelligence (AI)-based capabilities for border and coast guard applications*. Downloaded 2024, November 19, from https://www.frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf
14. Jones, C., Lanneau, R., & Maccanico, Y. (2023). *Europe's techno borders.* EuroMed Rights – Statewatch. Downloaded 2024, November 23 from https://www.statewatch.org/media/3964/europe-techno-borders-sw-emr-7-23.pdf
15. López, B.C. (2023). Border policing at sea: Tactics, routines, and the law in a Frontex patrol boat, *The British Journal of Criminology*. *63*(1), pp. 1–17. Downloaded 2024, November 25 from https://doi.org/10.1093/bjc/azac009
16. Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624. *OJ L*, 295/1, 2019
17. Ristić, V. (2022). The European Model of the Integrated Border Management. *Pravo – teorija i praksa*, *39*(2), pp. 91–107. https://doi.org/10.5937/ptp2202091R

18. Treaty of Lisbon (Treaty on European Union. 2016. Consolidated version). *OJ C* 202, 7. 7. 2016, pp. 1-389
19. Vasilkov, Z. (2023). *Unutrašnji poslovi i bezbednost u pravu Evropske unije nakon Lisabonskog ugovora* [*Internal affairs and security in the law of the European Union after the Treaty of Lisbon*]. Beograd: Zadužbina Andrejević

Marković M. Darko[*]
https://orcid.org/0000-0001-9124-6417
Marković Darija[**]
https://orcid.org/0000-0001-5602-902X

UDK: 343.326:004
Original scientific paper
DOI: 10.5937/ptp2502049M
Received on: April 8, 2025
Approved for publication on:
April 29, 2025
Pages: 49–61

CYBERCRIME AND LAW – MANAGING CHALLENGES AND PROSPECTS IN THE DIGITAL AGE

ABSTRACT: Cybercrime has emerged as a global threat in the digital age, posing significant challenges to legal systems worldwide, particularly in terms of their effectiveness and applicability. This paper examines how these challenges are addressed within international and national legal frameworks, highlighting key obstacles and offering perspectives for improvement. It reviews existing legal mechanisms, such as the Budapest Convention, the General Data Protection Regulation (GDPR), and national legislation in Serbia, and evaluates their adaptability to contemporary technological threats and potential for reform. The research adopts an interdisciplinary methodology, combining theoretical analysis of international and domestic legal texts with empirical examination of statistical data and case records. Practical challenges of legal enforcement are assessed through a systematic review of relevant sources, including the number of reported cyberattacks, and insights drawn from Interpol and Europol reports.

The findings highlight systemic challenges, such as jurisdictional limitations, ineffective laws, and insufficient technical capacities. Proposed solutions emphasize enhanced international cooperation, modernization

[*] PhD, Associate Professor, University Business Academy in Novi Sad, Faculty of Law for Commerce and Judiciary in Novi Sad, Novi Sad, Serbia, e-mail: darko.markovic@pravni-fakultet.edu.rs

[**] Msc, PhD candidate, RUDN University, Law Institute, Moscow, Russia, e-mail: darija.dm.markovic@gmail.com

of legal frameworks, investment in technology, and public education. The paper concludes that building legal resilience to cybercrime requires a coordinated international effort to address legal and technological vulnerabilities exploited by cybercriminals.

Keywords: *cybercrime, law, digital age, jurisdiction, international cooperation.*

1. Introduction

When thinking about cybercrime, it is simply unthinkable not to see how much of a daily risk it has become – it is no longer a question of if it will happen, but when. Cybercriminals aren't just someone breaking into your computer and taking your password; it's a whole world of fraud, theft, and even endangering the security of countries. In order to even discuss what cybercrime is, one must first clarify what is included in that term. In a general interpretation, cybercrime includes malicious activities such as identity theft, unauthorized access to personal data and their misuse for the purpose of false representation, for example with the aim of stealing money or taking a loan on the account of the victim. Phishing is a widely known concept – e-mail users often receive e-mails that "inform" them that they must submit their account information, while banks warn them not to fall for such scams. Ransomware is an insidious threat – the hacker locks files and demands a ransom, and if the victim doesn't pay, they lose everything. DDoS attacks flood the server with requests until the site goes down, and social media scams involve fake messages that trick the user into clicking on a malicious link.

According to a report by Cybersecurity Ventures, the global cost of cybercrime is expected to reach $10.5 trillion annually in 2025, three and a half times more than in 2015 (Esentire, 2024) – that's more than the GDP of many countries! Ransomware attacks are sometimes taken lightly, on the principle of "it's not me, who cares about me". Nevertheless, it is a danger that is spreading, growing from year to year, and practically no one can be sure that he will not be the subject of such an attack and blackmail tomorrow. In the last five years, this risk has increased by numbers that are equally ruthless – the number of these attacks has increased by as much as 150% in the period from 2020 to 2025 (Griffiths, 2025). What does this mean in practice? That every day at least one company or at least one individual is a victim of such an attack. Or, more precisely, it happens every 14 seconds (Palatty, 2025). One in a sea of examples of such criminal acts occurred in

2021 in the USA, when hackers broke into the Colonial Pipeline system and locked it, then demanded a ransom, and while waiting for a solution to this problem, there was a fuel shortage on the East Coast (Easterly & Fanning, 2023). Or the Facebook data breach in 2023, when millions of users' data was leaked to the dark web (Behera, 2023). One might ask: "What's the use of my data, I'm not a famous person on the Internet". The answer could be quite unpleasant, just like in the aforementioned attack in 2023, when "unknown" people were also sent fake messages for months, causing them to lose money. These cases highlight the turbulence that cybercrime can cause in an individual's personal life or the functioning of a state. The financial losses are enormous – companies lose billions, and individuals often lose everything they have. However, those who have found themselves in similar predicaments know that it is not just about money. Because how can you pay for that feeling that someone, and not just anyone but a criminal, stole your identity and took away your privacy? The threat to national security is far more extensive, because the consequences are also more severe, often on a huge scale, as happened in the case of the attack on Estonian servers in 2007 (see Samsoerizal, Hidayat & Sukendro 2022). We have a drastic example of such attacks in the locking of hospital computer systems by hackers during the 2020 pandemic (He, Aliyu, Evans, & Luo 2021). Who can say in such moments that it is only about money when human lives are at stake? With all of this in mind, it's not hard to see that cybercrime isn't just a technical problem – it's a social problem, changing the way we trust each other, how we function as a community, and even how countries protect their citizens. With all these figures and cases, the question remains – how to deal with this, when everything happens at the speed of light, and criminals are always at least one step ahead?

Legal systems struggle with great restrictions when trying to react to this threat. Among the difficulties include the multinational character of cybercrime, obsolete legislation, technological backwardism, and the clash between privacy and security. The purpose of this paper is to investigate how current legal systems handle these issues, spot main challenges and provide fixes. Combining statistical data and case studies with the analysis of national and international legal actions, the study uses an interdisciplinary approach. Along with reports from agencies like Interpol and Europol, the methodological process consists in an examination of pertinent materials including the Budapest Convention, GDPR and national legislation of Serbia. By considering the legal frameworks and obstacles in their application, the aim of the paper is to help find solutions by which the law could more successfully control cybercrime..

2. Legal frameworks for cybercrime

If any crime is a global threat, then the same can be said for cybercrime, which increases the importance of establishing appropriate legal mechanisms. This need exists because the existing legal mechanisms are not sufficiently developed due to the major limitations of legal systems, primarily in terms of enforcement and efficiency. Perpetrators, their victims and infrastructure are often under different jurisdictions, and the international nature of these crimes poses a key burden in the search for applicable solutions. By studying current national and international legal systems, we can see the complexity of these issues, but also see directions in which we could go further.

Adopted in 2001 by the Council of Europe, the Convention on Cybercrime, sometimes known as the Budapest Convention (Council of Europe, 2001), is one of the main international papers for the fight against cybercrime. This agreement compels participating governments to enact legislation that prohibit illegal access to computer systems, data theft, computer fraud and similar crimes, therefore being the first attempt to create a shared legal framework to combat cybercrime. The Convention underlines especially the value of international collaboration in investigations, including information exchange and extradition. More than 70 states, including Serbia, which joined in 2009, had signed this convention by the beginning of this year. However, major challenges remain. Unfortunately, the global system is seriously compromised by the fact that large countries like China and Russia are not signatories, and past practice tells us that massive cyberattacks have often been linked to their infrastructures or citizens. Furthermore, the Budapest Convention was approved more than twenty years ago at a period when major ransomware assaults, the dark web, and cryptocurrencies were inconceivable. This begs the issue of whether this paper can handle contemporary problems include tracing anonymous bitcoin transactions or defending against attacks on important infrastructure.

Extra legal tools have been created inside the European Union to strengthen the battle against cybercrime. Adopted in 2016 and entered into force in 2018, the General Data Protection Regulation (GDPR) set rigorous criteria for the protection of user privacy (European Parliament and Council, 2016), therefore requiring businesses to guarantee the security of personal data. Regarding data leaks, the fines are substantial; for instance, a technology corporation in Ireland paid 1.2 billion euros for poor customer data protection in 2023 (Beveridge, 2023). But GDPR's main focus is safeguarding privacy, not actively fighting cybercrime, which restricts its applicability in this sense.

On the contrary, the NIS2 Directive, adopted in 2022 and approved in 2023, seeks to enhance the cyber security of EU vital infrastructure like hospitals, electricity grids and water systems. This directive mandates member states create national plans guaranteeing a quick reaction to events and safeguarding against cyberattacks. The NIS2 Directive's implementation is challenging, nevertheless; many nations – including certain EU members – have limited resources, specialists, and technical capacity to carry out these policies, therefore impeding development.

Legal actions pertaining to cybercrime exist in Serbia at the national level, however their efficacy is dubious. The 2016 Law on Information Security mandates public organizations and businesses to create mechanisms to stop cyberattacks and lays down guidelines for data protection. Article 301 of Serbia's Criminal Code forbids illegal access to a computer system, with a penalty of up to five years in prison, therefore addressing computer fraud. Still, the application of these rules runs several challenges. The absence of skilled staff is one of the main issues; in Serbia, there are few forensic professionals qualified to carry out thorough investigations about cybercrime. Furthermore, courts sometimes lack understanding of the technological features of these cases; how would you explain to a judge what blockchain is or how bitcoin transaction monitoring operates? This gets even more difficult when the perpetrators are from aboard since the Serbian court system lacks systems for efficient collaboration with other nations in such circumstances.

Variations in rules across countries present another major challenge. Imagine a situation where a Russian hacking group targets a German corporation using servers in the Netherlands, and the ransom money ends up in cryptocurrencies on a Singapore stock exchange. Which country has the jurisdiction to act and pass judgment? Germany, because its corporation is the victim? Russia, because the hackers are operating from where? The Netherlands, because its servers were used? Or Singapore, because the money landed there? Until countries agree on this, the perpetrators usually disappear without a trace. Europol said in 2024 that a large number of cyberattacks still go unsolved, mainly because of these problems: hackers mask their actions using VPNs, the dark web, anonymous payment methods (Eurojust & Europol, 2024). This highlights a fundamental flaw in legal systems designed for the physical world, where the identity of the perpetrator is evident, but in the digital sphere such barriers do not exist and traces are easily erased. Although they provide the foundation for combating cybercrime, legal systems have major limitations that require fresh ideas and adaptation to modern technical issues.

3. Challenges in the fight against cybercrime

Cybercrime is one of the most complex threats of our time, and legal systems globally encounter several challenges in attempting to combat it. Another fact, at this time, is that while technology continues to advance rapidly, legislation and law enforcement mechanisms are usually years behind and the criminals work in the shadows with the greatest ease (Marković & Zirojević, 2024). An examination of these difficulties shows deep-seated structural and practical challenges, from jurisdictional complications to a lack of technical expertise, that collectively hinder the effective fight against this global menace.

One of the most serious hurdles in fighting cybercrime is jurisdiction. Cyber attacks are not limited by geography – the actor in one country, the infrastructure used for the attack in a second, the victim in a third. For instance, a Chinese hacker can hack the server of an American company using an intermediary server in Brazil, while the ransom for the ransomware should be paid via cryptocurrency through the Dubai stock exchange. What country has jurisdiction to investigate and prosecute this case? China because the hacker is located there? America, because the victim is on my side there? Brazil, because it was how its infrastructure was used? Or Dubai, since the money went there? These are not just hypothetical questions – we have sen in the Europol report that the majority of cyber attacks go unsolved for exactly these jurisdictional reasons (Eurojust & Europol, 2024). Hackers are signing up for VPNs, working on the dark web and making anonymous payments to cover their tracks, leaving judicial authorities in a stalemate over who has jurisdiction (more details in Zirojević & Ivanović, 2021).

Another major problem is the law becoming old. Many cybercrime laws were already written decades ago, long before the Internet enjoyed the status it enjoys today. One example can be from our country, Serbia, where the Law on Information Security was adopted in 2016, but this law and the Criminal Code have not been significantly updated in that context since then, which has led to provisions that do not reflect modern forms of cybercrime (forexample mass ransomware attacks, etc., as well as the misuse of artificial intelligence to create false identities). Other countries share the same fate – the US still utilizes the Computer Fraud and Abuse Act of 1986, vintage from an era when few owned computers and the Internet was fresh, to prosecute cybercriminals. Such legislation is generally not well equipped to tackle modern threats, likethe tracing ofotherwise untraceable bitcoin transactions or preventing attacks on critical infrastructure through advanced botnets.

We encounter another hurdle in the technological backwardness of judicial systems. Many police, prosecutors and courts lack the tools to monitor cyber attacks. Tracking fraud transactions, for instance, calls for specialized software and knowledge of blockchain technology yet that is not exactly the case in Serbia, the majority of police agencies there lack even fundamental resources for such a task. Police officers in Europe are not sufficiently trained to deal with large amounts of data in cybercrime investigations, and it can be said that they lag behind technology, which is why they have many problems in the field of digital forensics (Muncaster, 2025). The courts complicate things further – judges often don't have the technical skills to evaluate seemingly arcane evidence, like server logs or messages encrypted from the dark web.

Furthermore, there is tension between privacy and security (Domazet, Marković & Skakavac, 2024), complicating efforts to combat cybercrime. Regulations similar to GDPR in the E.U., while important to privacy (Mladenov, 2023), impose tight constraints on data collection and sharing, slowing investigations. For example, if the police want to obtain user data from a technology company, they must complete complex procedures to comply with the GDPR, giving criminals an opportunity to cover their tracks. Meanwhile, the likes of Apple and WhatsApp employ end-to-end encryption for their messages, enabling them not even to access user content, even when police demand it. This led to a worldwide debate – the British government fought in 2024 to start a campaign to outlaw end-to-end encryption, claiming it obstructed inquiries into cybercrime, but faced stiff resistance from privacy activists, who argued that this would infringe users' basic rights (Szóka & Boulton, 2025).

There aren't many experts in forensic science who have some knowledge of cybercrime, especially not in a place like Serbia, where salaries in the public sector are paltry and private companies can provide better working conditions.

Experts estimated four years ago that there will be a shortage of 3.5 million cyber professionals in 2025, three and a half times more than in 2013, which is staggering, but in judicial institutions, it is very glaring (Morgan, 2021). The police can't follow digital trails and the courts can't make sense of the evidence without specialists' help. Thus, they can find themselves in a position to absolve a hacker who steals data from a hospital system, a bank or even from government servers – simply because they do not have an expert who can confirm the authenticity of the digital evidence. These are challenges that remind us of the need of a transformational change of our legal system. Cybercrime is not merely a technical issue – it needs global cooperation, new

laws, investment in technology and training of specialists (Matijašević & Dragojlović, 2021). Without it, justice systems are always one step behind criminals who use the anonymity and speed afforded by the digital age to dodge justice.

4. Perspectives and solutions

It needs a holistic and synergistic approach towards cybercrime as existing laws systems have proved with limited success combatting this global threat. Indicators for the future related for example to international cooperation, modernization of laws, investments in technology and public education have been drawn on the basis of the analysis presented.

International cooperation is the starting point tackling cybercrime more effectively. The Budapest Convention is powerful but should be expanded to other countries, with key global actors like Russia and China missing from this framework and forming significant holes in the system. In this regard, the UN Agreement on Cybercrime (Council of Europe, 2025) can serve as an important enabler in this wider framework of cooperation. States should align their legislation and facilitate information sharing so that perpetrators can be swiftly tracked down and prosecuted, no matter where jurisdiction lies.

Equally important is the modernization of national laws. The two legal acts, the Law on Information Security and the Criminal Code, need to be harmonized with modern threats, such as ransomware attacks and cryptocurrency abuse. By way of example, provisions that would trace the anonymous cryptocurrency transactions would mean much more could be traced. Similarly, countries such as the US would have to reform archaic legislation such as the Computer Fraud Act of 1986, in order for such laws to include new types of cybercrime (Berris, 2020), including abuse of artificial intelligence.

Technological advances are no end of the answer to the backwardness of many law enformcements. Acquiring specialized digital trail tracing tools – like software for analyzing blockchains – would help police and courts to prosecute criminals more efficiently. Forensic experts need to be trained – estimates of the lack of 3.5 million cyber security experts are certainly worrying, and Serbia is particularly vulnerable in this regard. To address this gap, states need to invest in the education and employment of experts.

Public education is a major component of prevention. It helps reduce the number of victims, as exemplified by Internet safety campaigns – e.g. a good practice example is Estonia (Holm, 2025) – through the use of e-government

and training of citizens, this country has greatly decreased cybercrime. A similar approach could be followed in Serbia, where users' awareness of digital threats is still low.

Finally, the great news is that artificial intelligence is also being applied to detect and prevent cyberattacks. Artificial intelligence tools can recognize attack patterns and predict them, but there is also a risk of misuse, so additional guidelines are needed for their use. The answer to this lies in a level of global co-ordination, advancements in tech and education – and only then can we hope the law will be able to keep up with the cybercriminals.

5. Conclusion

Cybercrime in the digital age has emerged as a global scourge, a threat that legal systems around the world have had difficulty addressing, and this study identifies important challenges and potential avenues for reform. Based on the theoretic review of international and national legal framework it can be concluded that existing mechanisms (Budapest Convention, GDPR) provide a basis for cybercrime fighting, however, they are constrained by inconsistency of legal frameworks in relation of the countries and ways of modern technologies. Law on Information Security and the Criminal Code regulate the field in Serbia, but implementation is one step behind due to the absence of experts and technical capacity. Difficulties like jurisdictional complexity, technology lag, and privacy versus security also make an effective response difficult – Europol reported in 2024 that most cyber attacks go unresolved, primarily due to the anonymity facilitated by VPNs and the dark web.

It is necessary to take a holistic approach in order to combat cybercrime. The Budapest Convention should be expanded to include more countries, and countries like Russia and China should be included in global agreements. This will help promote international collaboration. National legislation must be modernized to deal with current threats like ransomware attacks and the use of cryptocurrencies. Educating the public, training forensic experts and providing specialized tools for the police and courts is the next step towards uncovering new digital clues. And privacy and security must be reconciled – lawmakers have to strike the balance between wanting to protect user data and enabling effective investigations. The future includes international treaties such as the UN Cybercrime Treaty and the application of artificial intelligence to detect and prvent attacks, but till then the cybercriminals are one step ahead of justice without global coordination and tech advances.

Marković M. Darko
Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, Srbija

Marković Darija
Univerzitet RUDN, Pravni institut, Moskva, Rusija

KIBERNETSKI KRIMINAL I PRAVO – UPRAVLJANJE IZAZOVIMA I PERSPEKTIVAMA U DIGITALNOM DOBU

APSTRAKT: Kibernetski kriminal u digitalnom dobu se pojavio kao globalna pretnja koja izaziva pravne sisteme širom sveta sa višestrukim ograničenjima efikasnosti i primenljivosti. Istražujemo kako se ovi izazovi rešavaju u međunarodnim i nacionalnim pravnim okvirima, naglašavamo ključne prepreke i pružamo perspektive za unapređenje. U radu se pokušavaju sagledati postojeći pravni mehanizmi, uključujući Budimpeštansku konvenciju i GDPR i nacionalne zakone u Srbiji, kao i njihova prilagodljivost savremenoj tehnološkoj pretnji i mogućnostima za reformu. Ovo istraživanje je zasnovano na interdisciplinarnoj metodologiji, kombinujući teorijsku analizu međunarodnih i domaćih pravnih tekstova sa činjeničnim proučavanjem statističkih podataka i evidencije slučajeva. Praktični izazovi sprovođenja zakona se procenjuju kroz sistematsko raščlanjivanje relevantnih izvora, uključujući broj prijavljenih slučajeva sajber napada, izveštaje Interpola i Evropola u kojima se daju uvidi u određene slučajeve. Nalazi naglašavaju sistemske izazove, kao što su ograničenja u nadležnostima, neefikasni zakoni i nedostatak tehničkih kapaciteta, dok rešenja ukazuju na veću međunarodnu saradnju, modernizaciju zakona, ulaganje u tehnologiju i javno obrazovanje. Rad dolazi do zaključka da bi trebalo da postoje koordinisani međunarodni napori da se poboljša pravna otpornost na kibernetski kriminal, kako bi se prodrlo kroz sajber zidove koji štite kriminalce.

Ključne reči: *sajber kriminal, pravo, digitalno doba, jurisdikcija, međunarodna saradnja.*

References

1. Behera, S. K. (2024). The Facebook data breach and its consequences for consumer privacy and cybersecurity. *National Journal of Cyber Security Law*, *7*(1), pp. 1–6
2. Berris, P. G. (2020). *Cybercrime and the law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress*. Congressional Research Service. Downloaded 2025, March 14 from https://www.congress.gov/crs_external_products/R/PDF/R46536/R46536.3.pdf
3. Beveridge, C. (2023). Irish Data Protection Commissioner imposes a €1.2 billion fine on Meta Ireland. *BDO Global Portal*. Downloaded 2025, February 28 from https://www.bdo.co.uk/en-gb/insights/advisory/risk-and-advisory-services/irish-data-protection-commissioner-imposes-a-1-2-billion-fine-on-meta-ireland
4. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986).
5. Council of Europe. (2024). *United Nations treaty on cybercrime agreed by the Ad Hoc Committee*. Council of Europe Portal. Downloaded 2025, March 15 from https://www.coe.int/en/web/cybercrime/-/united-nations-treaty-on-cybercrime-agreed-by-the-ad-hoc-committee
6. Council of Europe. (2001). *Convention on Cybercrime* (European Treaty Series No. 185). Budapest, Hungary. Downloaded 2025, March 15 from https://rm.coe.int/1680081561
7. Domazet, S., Marković, D. M., & Skakavac, T. (2024). Privacy under threat – The intersection of IoT and mass surveilance. *Pravo – teorija i praksa*, *41*(3), pp. 109–124. DOI:10.5937/ptp2403109D
8. Easterly, J., & Fanning, T. (2023). *The attack on Colonial Pipeline: What we've learned & what we've done over the past two years*. CISA America's Cyber Defense Agency. Downloaded 2025, March 14 from https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years
9. eSentire. (2024). *Cybersecurity Ventures report on cybercrime*. eSentire. Downloaded 2025, March 5 from https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime
10. European Parliament and Council. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)* (Official Journal of the European Union, L 119/I of 4 May 2016). Downloaded 2025, February 28 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

11. Griffiths, C. (2025). *The latest 2025 ransomware statistics (updated January 2025)*. AAG. Downloaded 2025, March 5 from https://aag-it.com/the-latest-ransomware-statistics/
12. He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health care cybersecrutiy challenge and solutions under the climate of COVID-19 scoping review. *Journal of Medical Internet Research*, *23*(4), e21747. DOI: 10.2196/21747
13. Holm, P. (2025). *Estonia's bold approach to cyber security: A holistic model for Europe*. e-Estonia. Downloaded 2025, March 22 from https://e-estonia.com/estonias-cyber-security-model-for-europe/
14. Krivični zakonik [Criminal Code]. *Službeni glasnik RS*, br. 85/05, 88/05 – ispr., 107/05 – ispr., 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19 i 94/24
15. Marković, D. M., & Zirojević, M. (2024). Izazovi u regulisanju i identifikaciji deepfake sadržaja [Challenges in regulating and identifying deepfake content]. In: Počuča, M. (ed.), *XXI međunarodni naučni skup „Pravnički dani – Prof. dr Slavko Carić" Odgovori pravne nauke na izazove savremenog društva* [*XXI International Scientific Conference "Legal days – Prof. Slavko Carić, PhD" The responses of legal sciences to the challenges of modern society*] (pp. 679–692). Novi Sad: Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, DOI: 10.5937/PDSC24679M
16. Matijašević, J., & Dragojlović, J. (2021). Metodika otkrivanja krivičnih dela računarskog kriminaliteta [Methodology of detection of computer crime offenses]. *Kultura polisa*, *18*(2), pp. 51–63. DOI:10.51738/Kpolisa2021.18.2p.1.04
17. Mladenov, M. (2023). Human vs. Artificial intelligence – EU's legal response. *Pravo – teorija i praksa*, *40*(1), pp. 32–43. DOI:10.5937/ptp2300032M
18. Morgan, S. (2021). *Cybersecurity jobs report: 3.5 million unfilled positions in 2025*. Cybersecurity Ventures. Downloaded 2025, March 19 from https://cybersecurityventures.com/jobs-report-2021/
19. Muncaster, P. (2025). *European police: Data volumes and deletion hindering investigations*. Infosecurity Magazine. Downloaded 2025, February 28 from https://www.infosecurity-magazine.com/news/police-data-volumes-deletion/
20. Palatty, N. J. (2025). *How many cyber attacks per day: The latest stats and impacts in 2025*. Astra IT. Downloaded 2025, March 25 from https://www.getastra.com/blog/security-audit/how-many-cyber-attacks-per-day/

21. Samsoerizal, A. D., Hidayat, E. R., & Sukendro, A. (2022). Analytical study of Indonesian cybersecurity lesson learned from Estonian Cyberattacks in 2007. *International Journal of Arts and Social Science*, *5*(2), pp. 31–36. https://www.ijassjournal.com/2022/V5I2/414659927.pdf
22. Szóka, B., & Boulton, S. (2025). *UK encryption crackdown imperils privacy, security & free speech*. Tech Policy Press. Downloaded 2025, March 15 from https://www.techpolicy.press/uk-encryption-crackdown-imperils-privacy-security-free-speech/
23. Zakon o informacionoj bezbednosti [Law on Information Security]. *Službeni glasnik RS*, br. 6/16, 94/17, 77/19
24. Zirojević, M., & Ivanović, Z. (2021). *Cyber law – Serbia.* Belgrade: The Institute of Comparative Law

Veljković Sanela[*]
https://orcid.org/0009-0003-3650-290X

UDK: 623.454.8
Original scientific paper
DOI: 10.5937/ptp2502062V
Received on: February 21, 2025
Approved for publication on:
April 24, 2025
Pages: 62–74

ORIENTALISM AS A FACTOR IN THE DEVELOPMENT OF INTERNATIONAL LAW ON NUCLEAR SECURITY

ABSTRACT: Orientalism refers to the discursive process through which Western societies construct a spatial imaginary of the "Orient" or the East. This conceptual framework can be useful in analyzing contemporary nuclear relations. The dichotomy between nuclear powers and Third World states stems directly from the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), whose provisions established which states were granted the status of nuclear powers. Consequently, all other countries—those that did not possess nuclear weapons at the time the treaty was adopted—were denied such a status.

In the decades that followed, several Third World states developed their own nuclear programs, including India, Pakistan, North Korea, Israel, and Iran. Some of these countries never accepted the provisions of the NPT, while others later withdrew from the obligations they had undertaken. This paper investigates the role of Orientalism as a contributing factor in the development of international law on nuclear security. It analyzes how Orientalist viewpoints have shaped the formation of international legal norms, with particular emphasis on their disproportionate effects on Third World states. The paper concludes by underscoring the need to reassess existing paradigms in international relations in order to reduce geopolitical tensions and enhance global nuclear security.

[*]MSc, Junior Research Assistant, University of Belgrade – 'Vinča' Institute of Nuclear Sciences, National Institute of Importance for the Republic of Serbia, Belgrade, Serbia, e-mail: sanela.veljkovic@vin.bg.ac.rs

***Keywords**: nuclear orientalism, nuclear weapons, the West, Third World states.*

1. Introduction

Throughout human history, nuclear weapons have been used twice – to bring an end to World War II. The bombings of Hiroshima and Nagasaki in 1945 demonstrated the devastating power of nuclear weapons. The consequences were not only immediate in terms of human and material losses but also had lasting effects in the years that followed. The Cold War ensued, named precisely because the two nuclear superpowers – the United States and the Soviet Union – possessed weapons of mass destruction but did not use them. The strategy of deterrence proved effective, and while nuclear weapons continued to be developed and refined, they were not deployed in conflicts. During the Cold War, two additional European countries began developing their own nuclear programs. The United Kingdom conducted its first nuclear test in 1952, followed by France in 1960. Shortly after these successful tests by European states, the People's Republic of China became the fifth country to successfully carry out nuclear testing in international relations. In 1968, the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) was adopted. The treaty established rights and obligations for states that had already developed nuclear weapons as well as for those that had not. However, some countries – India, Pakistan, and Israel – chose not to accept the treaty. Each of these nations cited different political, military, and security concerns as reasons for their rejection. On the other hand, North Korea, despite being a signatory to the NPT, withdrew in 2003 and subsequently began conducting nuclear tests. Although Iran remains a signatory, there are significant concerns that it is developing nuclear capabilities for military purposes. These states do not hold the status of nuclear powers and are not part of the "Nuclear Club" – a group consisting of the five states that possessed nuclear weapons at the time of the NPT's adoption. A direct consequence of the NPT has been the emergence of a new (nuclear) dimension in the dichotomy between the West and the East in international relations. The objective of this paper is to explore and analyze this dichotomy as it exists in contemporary nuclear relations. Accordingly, the methodological approach is based on the qualitative analysis of relevant legal, political, and theoretical sources. Using the historical-comparative method, the development of nuclear programs in different states is analyzed, while discourse analysis is employed to understand how orientalist stereotypes are manifested and sustained in contemporary international nuclear security law.

To that end, the first section of the paper introduces the concept of Orientalism. The second section focuses on the development of nuclear programs during the Cold War and major initiatives in the post-Cold War era. The third section examines how Orientalism manifests in contemporary nuclear relations. Finally, the paper concludes with key findings and includes a list of references used in the research.

2. Edward Said's Orientalism

The process of constructing and reinforcing one's own identity in relation to the Other has been present throughout human history. While the Other is often characterized as backward, rural, and uncivilized, the Self is portrayed with diametrically opposite qualities. Various dichotomies have existed, among which the West-East divide appears to be the most dominant. Historically, this divide has applied to societies that coexisted but differed in political, religious, or cultural terms (Todorova, 2006, p. 61). In his 1978 work Orientalism, Edward Said (2008) describes the British colonization of Egypt from 1882 to 1914. The concept of Orientalism is best illustrated through a speech by Arthur Balfour and the Earl of Cromer, a British politician and consul in Egypt, stating: "We are not in Egypt only for the Egyptians, although we are there for them; we are also there for Europe as a whole" (p. 48). Here, ruling over the Other is presented as a service – something that benefits not only the Egyptians but also the Europeans. The characteristics attributed to the Other, in this case, the Egyptians, serve to legitimize British control over Egypt.

Orientalism is often equated with colonialism, which was a dominant practice in the 19th century. However, Orientalism is a more enduring discourse, with colonialism being just one of its many manifestations, albeit the most well-known (Tepšić & Vukelić, 2019). Similarly, Patrick Geary (2007) notes that Orientalism as a discourse dates back to antiquity or biblical times when societies were divided into two groups – those considered constitutive and biological or civilized and barbaric. The concept of Orientalism also shares similarities with humanitarian interventionism. Within this discourse, the West is seen as progressive, and "(...) given that we produce abundantly and possess so many rights in the West, we must find markets to which we can export these products and rights" (Duzinas, 2009, p. 118). The relationship between the West and the Other, in this case, can also be viewed as a variation of Orientalism or as a "relationship between a weak and a strong partner" (Said, 2008, p. 57). Over time, some scholars have discussed the reproduction

of Orientalism, a concept that seeks to explain various discourses from the former Yugoslavia in the 1990s. This concept suggests that post-Yugoslav states, having themselves been Orientalized, began applying Orientalist discourse to their neighbors (Bakić-Hayden, 2006).

It is important, however, not to conflate the concept of Orientalism with similar discourses. Said (2008) offers three somewhat different explanations of Orientalism, while warning that they overlap. The broadest definition describes Orientalism as "a style of thought based on an ontological and epistemological distinction made between the Orient and (most often) the Occident" (p. 11). The academic definition considers an Orientalist to be any scholar who teaches, writes about, or researches the Orient, with Orientalism being the product of their work. Lastly, Said defines Orientalism as "a Western style of domination, restructuring, and possessing authority over the Orient" (p. 11). This conceptualization of Orientalism provides a foundation for examining other diverse practices and discourses in international relations. One of its variations is nuclear Orientalism, which will be discussed in the following sections. Before that, however, it is necessary to present the development of nuclear weapons and the initiatives aimed at nuclear disarmament.

3. From the first use of nuclear weapons to the present

To ensure the end of World War II, the United States used nuclear weapons. The consequences were enormous, not only in terms of human and material losses but also in their impact on the environment and public health. This was followed by a period known in history as the Cold War. Instead of open military conflict, the United States and the Soviet Union engaged in a competition for military technological advancement and an ideological struggle for influence over other states. Until 1949, when the Soviet Union successfully conducted its first nuclear test, the United States remained the only country in possession of nuclear weapons. The fact that both superpowers possessed nuclear weapons and that their potential use could result in mutual destruction led to the development of the concept of deterrence in international relations. Deterrence was based on "threatening the other side with nuclear retaliation should they cross a certain line perceived as endangering vital interests" (Trapara, 2012, p. 111). The closest moment to a nuclear conflict between the United States and the Soviet Union during the Cold War was the Cuban Missile Crisis of 1962.

In literature and international legal instruments, different definitions of nuclear weapons exist. The Treaty for the Prohibition of Nuclear Weapons

in Latin America and the Caribbean (1967) defines nuclear weapons as "any device capable of releasing nuclear energy in an uncontrolled manner and possessing characteristics suitable for use in armed conflicts. A means of transport or launching such a device is not included in this definition if it is separable from the device". Analyzing this definition, Professor Hrnjaz (2014) argues that a comprehensive definition must also include the means of delivery and methods of nuclear energy release. Meanwhile, some scholars differentiate between nuclear and atomic weapons, treating nuclear weapons as a subset that includes thermonuclear and neutron weapons (Manojlović, 2009). Others classify nuclear weapons as weapons of mass destruction due to the severe consequences of their use (See, for example: Panofsky, 998).

During the Cold War, various international legal instruments were adopted to regulate nuclear weapons. These include: the Partial Test Ban Treaty (1963), the Treaty on the Non-Proliferation of Nuclear Weapons (NPT, 1968), the Anti-Ballistic Missile (ABM) Treaty (1972), the Strategic Arms Limitation Treaties (SALT I, 1972 and SALT II, 1979). Additionally, international agreements established nuclear-weapon-free zones in Latin America and the Caribbean, the South Pacific, Southeast Asia, and Africa (For more details, see Goldblat, 1997; Raičević, 2000). Following the bombings of Hiroshima and Nagasaki and the realization of the devastating consequences of nuclear weapons, an anti-nuclear movement emerged during the Cold War. This movement criticized nuclear weapons development and testing, significantly influencing public opinion and political decisions regarding nuclear arms control.

Despite these efforts, the number of nuclear-armed states continued to grow in the 1950s and 1960s. The United Kingdom conducted its first nuclear test in 1952, followed by France in 1960 and China in 1964. When the NPT was adopted in 1968, these five states were recognized as nuclear-weapon states based on their possession of nuclear weapons at the time. The treaty obligated these states to reduce their nuclear arsenals, while non-nuclear-weapon states could only use nuclear energy for peaceful purposes. Despite the large number of signatories, India, Pakistan, and Israel refused to join the NPT, arguing that it effectively established a system of global "nuclear apartheid" (Gusterson, 2006, p. 2). North Korea, initially a signatory, withdrew from the treaty in 2003 and subsequently developed its nuclear program. Iran, although a signatory, has been subject to significant scrutiny due to suspicions that it is developing nuclear capabilities for military purposes.

One of the defining features of the post-Cold War era regarding nuclear weapons is the expansion of nuclear energy use – both for peaceful purposes

and in terms of increasing the quantity and quality of nuclear arsenals (Vukadinović, 2006, p. 130). Several major international agreements were adopted in this period: the Strategic Arms Reduction Treaty (START I, 1991), the Strategic Arms Reduction Treaty (START II, 1993), the Comprehensive Nuclear-Test-Ban Treaty (1996), the New START Treaty (2011), the Treaty on the Prohibition of Nuclear Weapons (2017). In 2009, the United Nations Security Council adopted Resolution 1887, emphasizing nuclear non-proliferation and disarmament efforts. The legality of nuclear weapon use was brought before the International Court of Justice (ICJ) in the late 20th century. While the Court's conclusions were complex, they indicated that there is no absolute prohibition in international law against the use of nuclear weapons (For more details, see: Legality of the threat or use of nuclear weapons. Advisory opinion of 8 July 1996).

4. Orientalism in contemporary nuclear relations

The Treaty on the Non-Proliferation of Nuclear Weapons (NPT) establishes the rights and obligations of two groups of states: those that possess nuclear weapons and those that do not. A direct consequence of the treaty is that states attempting to develop nuclear weapons outside this framework are considered "rogue states; dangerous nations driven by passion and irrationality, the antithesis of rational, security-oriented nuclear-armed states" (Urwin, 2016, p. 239). Based on this perception, India, Pakistan, Iran, and North Korea are viewed as rogue states in contemporary nuclear relations. Meanwhile, Israel never accepted the 1968 treaty and did not officially confirm or deny the possession of nuclear weapons. However, the classification of Third World states as underdeveloped compared to the five recognized nuclear powers represents Said's Orientalism in a different context (Gusterson, 1999). Nuclear Orientalism is another variation of Orientalism, serving as a means to prevent nuclear proliferation. This is evident in the fact that the NPT granted nuclear power status to China and Russia – two historical victims of Orientalism (For more details, see, for example: Nojman, 2011). The Western members of the Nuclear Club have skillfully used nuclear Orientalism to deny states that had not developed nuclear weapons before 1968 the opportunity to become "legitimate" nuclear actors.

This nuclear Orientalism is based on four assumptions (Gusterson, 2006): Third World countries are too poor to afford nuclear weapons; Deterrence in the Third World is inherently unstable; Third World governments lack the technical competence to manage nuclear weapons; Third World regimes lack

the political maturity to be trusted with nuclear weapons. The relationship between the five recognized nuclear powers and Third World states can be described as "police over criminals, men over women, and adults over children" (Gusterson, 1999, p. 131). When discussing Third World states and nuclear weapons, two common fear-inducing narratives emerge: Terrorist groups will acquire nuclear weapons and use them to harm the West; A nuclear incident in the Third World will trigger World War III (Williams, 2011). These scenarios stem from perceptions that Third World states are too anarchic and underdeveloped to regulate their internal affairs, let alone guarantee the security of their nuclear infrastructure. However, it is crucial to consider the political and social specificities of each so-called rogue state in contemporary nuclear relations.

India justified its first nuclear test by invoking the idea of "nuclear apartheid" – a reference to the ongoing exclusion and marginalization of non-Western nations in a global order dominated by privileged Western states (Biswas, 2001, p. 495). India's relationship with Pakistan is highly complex. These two countries have a long history of hostility and frequent conflicts, further complicated by the fact that both possess nuclear weapons. Their nuclear capabilities significantly impact regional geopolitical dynamics, reinforcing a strategy of deterrence in South Asia. For Pakistan, several red lines must not be crossed by India: Invasion and occupation of a significant portion of Pakistan, destruction of most of Pakistan's land and air forces, a blockade significantly reducing Pakistan's supplies, and political destabilization of Pakistan; unofficially, threats to Pakistan's control over its part of Kashmir and attacks on its nuclear facilities (Liebl, 2009). According to Šabanić (2016), if regional and international tensions continue to escalate alongside Pakistan's internal instability, there is a significant likelihood of a fifth war between India and Pakistan, which would have global repercussions. A nuclear exchange in such a conflict would have catastrophic global consequences.

Although North Korea signed the NPT in 1968, it withdrew in 2003. Some scholars argue that North Korea's nuclear weapons program is driven by "the desire of a closed and highly paranoid leadership to restart a military adventure against the South while using nuclear deterrence to prevent U.S. intervention" (Vukadinović, 2006, p. 7). North Korea conducted its first nuclear test in 2006, officially entering the group of nuclear-armed states, but not the Nuclear Club. This is evident in UN Security Council Resolution 1718 (2006), which was passed in response to North Korea's test. Scholars have also examined the link between regime type and nuclear proliferation, concluding that "no democratic state without nuclear weapons has ever launched a secret nuclear program after

ratifying the NPT" (Sagan, 2011, p. 238). This aligns with the fact that North Korea's regime is classified as totalitarian and that its nuclear weapons program was likely developed in secrecy even while it was still an NPT member.

Iran's longstanding anti-Western stance has fueled U.S. concerns about its growing influence in the Middle East. Additionally, fears arise from Iran's alleged ties to various terrorist groups in the region and the fact that Iran's political system is fundamentally different from the Western model. This reflects the persistent Orientalist framework, where "(Western) secularism is celebrated as a marker of progressive modernity, made possible through the simultaneous construction and condemnation of (Third World) fundamentalism" (Biswas, 2002, pp. 200–201). Iran frequently blames the West for various incidents. For instance, several Iranian nuclear physicists were assassinated in bombings across Tehran, with Iran accusing the U.S. and Israel (Bubnjević, 2023, p. 300). In 2010, a cyberattack on Iran destroyed over 1,000 centrifuges and extracted sensitive information from its nuclear program (Putnik, 2022, p. 119). When it comes to containing Iran's nuclear program, a significant diplomatic initiative was the Joint Comprehensive Plan of Action (JCPOA), signed in 2015. However, three years later, the United States unilaterally suspended its implementation. Analyzing Iran's nuclear program, Stojanović (2022) argues that Iran has achieved the status of a latent nuclear power, which on the Middle Eastern geopolitical stage "contributes to strategic stability by breaking Israel's nuclear monopoly" (p. 204).

A particularly problematic aspect of Middle Eastern security is that Israel never signed the NPT. The state neither confirms nor denies possessing nuclear weapons, maintaining a policy of nuclear opacity – "the undeclared construction, possession, and/or proliferation of nuclear weapons" (Žirovčić, 2009, p. 91). Israel plays a key role in Middle Eastern security, particularly in countering Iranian influence and terrorist groups. The Israeli-Palestinian conflict, which has lasted for decades, has recently escalated into a war between Israel and Hamas in Gaza. This conflict is further complicated by Iran's indirect involvement, as Tehran provides political, military, and financial support to Hamas and other Palestinian groups. Iran views this support as part of its broader strategy to expand its influence in the Middle East and counter Israel and the United States. Given the heightened tensions, there is a real risk of regional escalation, particularly if Iran directly joins the conflict. The biggest concern is that Israel is widely believed to possess nuclear weapons, while Iran remains under intense international scrutiny over its nuclear program. If Iran successfully develops nuclear weapons, the balance of power in the Middle East could be significantly altered.

5. Conclusion

The consequences of nuclear weapon use became evident after 1945. Since then, nuclear weapons have not been deployed in conflicts, yet several states continue to possess them. The Treaty on the Non-Proliferation of Nuclear Weapons (NPT) granted nuclear-weapon status to states that had developed such weapons by 1968. At the same time, the treaty imposed restrictions on all other nations, limiting their use of nuclear energy to peaceful purposes. As a result, the only "legitimate" nuclear powers are the United States, France, the United Kingdom, Russia, and China. However, today there are also rogue states – countries that developed nuclear weapons after 1968. This status applies to India and Pakistan, two neighboring states engaged in territorial disputes. The primary concern is not only their classification as developing Third World countries but also the fear that any conflict between them could escalate into a nuclear confrontation. Similarly, North Korea holds rogue-state status in contemporary nuclear relations. In this case, the primary concern is North Korea's political system, which fundamentally differs from Western values. Finally, the most feared rogue state is Iran, a Middle Eastern country that has pursued an anti-Western policy for decades and seeks to expand its influence in the region. Iran's alleged ties to religious extremism and terrorist organizations further alarm Western nations. The situation is further complicated by the West's tacit approval of Israel's nuclear arsenal, particularly by the United States. This raises a critical question at the heart of nuclear Orientalism: Why can Israel possess nuclear weapons, but Iran cannot? It appears that nuclear orientalism serves as a tool used by the original Nuclear Club, particularly the United States, to justify the prevention of nuclear proliferation. It is simply another variation of Orientalism, reflecting the selective use of Orientalist arguments to serve geopolitical interests. The result of this nuclear Orientalism, particularly by the Western powers of the Nuclear Club, is evident in today's Middle Eastern crisis, where instability has persisted for decades. Israel possesses a nuclear arsenal and holds a unique strategic position in the region, while Iran continues to face international scrutiny regarding its nuclear program. With the ongoing conflict in Gaza between Israel and Hamas, tensions between Iran and Israel have escalated further. Recent developments, combined with provocative statements from leaders on both sides, have increased the likelihood of a larger regional conflict. Escalation remains a real possibility, with the potential to draw in neighboring states as well as Western powers – particularly the United States. The stakes are too high, considering the catastrophic consequences the world

witnessed in 1945, not only for Japan but for global security as a whole. In this regard, the political and practical implications of this research point to the need for reexamining the existing criteria of the international nuclear order, particularly in the context of applying double standards. Removing orientalist narratives from international nuclear security law is a key step toward establishing a fairer, and thus more sustainable, international order. Future research should include a deeper analysis of international discourses and perceptions of nuclear threats, especially from the perspective of Global South countries, in order to build a more inclusive and effective understanding of nuclear security in the contemporary world.

ACKNOWLEDGEMENTS

This work was carried out within the scientific research activities of the 'Vinča' Institute of Nuclear Sciences – an institute of national importance for the Republic of Serbia, funded by the Ministry of Science, Technology, and Innovation, grant number 451-03-136/2025-03/ 200017.

Veljković Sanela
Univerzitet u Beogradu, Institut za nuklearne nauke „Vinča", Beograd, Srbija

ORIJENTALIZAM KAO FAKTOR U OBLIKOVANJU MEĐUNARODNOG PRAVA O NUKLEARNOJ BEZBEDNOSTI

APSTRAKT: Orijentalizam predstavlja diskurzivan proces konstrukcije prostornog imaginarijuma, odnosno Orijenta ili Istoka od strane zapadnih društava. Stoga, orijentalistička matrica može biti korisna u sagledavanju savremenih nuklearnih odnosa. Kada se govori o nuklearnoj proliferaciji, dihotomija nuklearne sile – države Trećeg sveta predstavlja direktnu posledicu Ugovora o neširenju nuklearnog oružja. Odredbe Ugovora definisale su kojim državama pripada status nuklearnih sila. Samim tim, sve ostale zemlje, odnosno one koje nisu posedovale nuklearno oružje prilikom usvajanja Ugovora nisu imale pravo na takav status. Međutim, pojedine države Trećeg sveta su narednih decenija razvile svoje nuklearne programe. U tu grupu država spadaju Indija, Pakistan, Severna Koreja,

Izrael i Iran. Neke od njih nikada nisu prihvatile odredbe Ugovora o neširenju nuklearnog oružja, dok su pojedine obustavile obaveze preduzete Ugovorom. Rad teži da istraži ulogu orijentalizma kao faktora u oblikovanju međunarodnog prava o nuklearnoj bezbednosti. S tim u vezi, analizira se uticaj orijentalističkih stavova na formiranje međunarodnih pravnih normi, s posebnim fokusom na njihove disproporcionalne efekte na države Trećeg sveta. Zaključak rada ukazuje na neophodnost preispitivanja postojećih paradigmi u međunarodnim odnosima kako bi se smanjile geopolitičke tenzije i poboljšala globalna nuklearna bezbednost.

Ključne reči: *nuklearni orijentalizam, nuklearno oružje, Zapad, države Trećeg sveta.*

References

1. Bakić-Hejden, M. (2006). *Varijacije na temu Balkana* [*Variations on the Balkan theme*]. Beograd: Filip Višnjić
2. Biswas, S. (2001). "Nuclear apartheid" as political position: race as a postcolonial resource? *Alternatives, 26*(4), pp. 485–522. DOI: https://doi.org/10.1177/030437540102600406
3. Biswas, S. (2002). The 'New Cold War': Secularism, orientalism, and postcoloniality. In: *Power, Postcolonialism and International Relations: Reading Race, Gender and Class* (pp. 184–208). London and New York: Routledge. Downloaded 2025, January 10 from: https://ir101.co.uk/wp-content/uploads/2017/11/biswas-the-new-cold-war.pdf
4. Bubnjević, S. (2023). *Alhemija bombe: prva i sveobuhvatna istorija nuklearnog doba* [*Alchemy of the bomb: The first and comprehensive history of the nuclear age*]. Beograd: Laguna.
5. Duzinas, K. (2009). *Ljudska prava i imperija: politička filozofija kosmopolitizma* [*Human rights and empire: The political philosophy of cosmopolitanism*]. Beograd: Službeni glasnik
6. Giri, P. (2007). *Mit o nacijama: srednjovekovno poreklo Evrope* [*The myth of nations: The medieval origins of Europe*]. Novi Sad: Cenzura
7. Goldblat, J. (1997). Nuclear-weapon-free zones: A history and assessment. *The Nonproliferation Review*, *4*(3), pp. 18–32
8. Gusterson, H. (1999). Nuclear weapons and the other in the Western imagination. *Cultural Anthropology, 14*(1), pp. 111–143. DOI: https://doi.org/10.1525/can.1999.14.1.111

9. Gusterson, H. (2006). A Double Standard on Nuclear Weapons?. *MIT Center for International Studies Audit of the Conventional Wisdom, 6*(8), pp. 1–5. Downloaded 2025, January 10 from: https://cis.mit.edu/sites/default/files/images/gusterson_audit.pdf
10. Hrnjaz, M. (2014). Legalnost upotrebe nuklearnog oružja u oružanim sukobima: ograničenja u vezi sa zaštitom čovekove životne sredine [The legality of the use of nuclear weapons in armed conflicts: Restrictions in relation to environmental protection]. *Godišnjak Fakulteta političkih nauka, 8*(12), pp. 115–132. DOI: 10.5937/GodFPN1412115H
11. Legality of the threat or use of nuclear weapons. Advisory opinion of 8 July 1996. International Court of Justice; Downloaded 2025, January 10 from: https://www.icj-cij.org/sites/default/files/case-related/95/095-19960708-ADV-01-00-EN.pdf
12. Liebl, V. (2009). India and Pakistan: competing nuclear strategies and doctrines. *Comparative strategy, 28*(2), pp. 154–163. DOI: https://doi.org/10.1080/01495930902799731
13. Manojlović, S. (2009). Međunarodno pravo i dozvoljenost upotrebe atomskog oružja [International law and the legality of the use of atomic weapons]. *Strani pravni život, 3,* pp. 351–368. Downloaded 2025, January 10 from: http://ricl.iup.rs/1275/1/document%20%2817%29.pdf
14. Nojman, I. (2011). *Upotrebe Drugog: Istok u formiranju evropskog identiteta* [*Uses of the Other: The East in the Formation of European Identity*]. Beograd: Službeni glasnik.
15. Panofsky, W. K. (1998). Dismantling the Concept of 'Weapons of Mass Destruction'. *Arms Control Today*, *28*(3), pp. 3–8
16. Putnik, N. (2022). *Sajber rat i sajber mir* [*Cyber War and Cyber Peace*]. Beograd: Inovacioni centar Fakulteta bezbednosti i Akademska misao
17. Raičević, N. (2000). Zone bez nuklearnog oružja [Nuclear-weapon-free zones]. *Zbornik radova Pravnog fakulteta u Nišu*, *40*(40-41), pp. 235–252
18. Sagan, S. D. (2011). The causes of nuclear weapons proliferation. *Annual Review of Political Science, 14,* pp. 225–244. DOI: http://dx.doi.org/10.1146/annurev-polisci-052209-131042
19. Said, E. (2008). *Orijentalizam* [*Orientalism*]. Beograd: Biblioteka XX veka
20. Stojanović, B. (2022). Sveobuhvatni (ne) sporazum: Iran kao nova nuklearna sila [The comprehensive (non)agreement: Iran as a new nuclear power]. *Nacionalni interes, 42*(2), pp. 185–209. DOI: https://doi.org/10.22182/ni.4222022.10

21. Šabanić, E. (2016). Povijest indijsko-pakistanskog sukoba [The history of the India-Pakistan conflict]. *Polemos: časopis za interdisciplinarna istraživanja rata i mira, 19*(37), pp. 121–136. Downloaded 2025, January 10 from: https://hrcak.srce.hr/file/250358.
22. Tepšić, G., & Vukelić, M. (2019). Kulturno nasilje kao proces dugog trajanja: od kolonijalizma do humanitarizma [Cultural violence as a long-term process: From colonialism to humanitarianism]. *Politička Misao: Croatian Political Science Review, 56*(1), pp. 109–131. DOI: 10.20901/pm.56.1.04.
23. Todorova, M. (2006). *Imaginarni Balkan* [*Imagining the Balkans*]. Beograd: Biblioteka XX vek
24. Trapara, V. (2012). Perspektive nuklearnog razoružanja u svetlu protivrečnih strategija nuklearnih sila [Perspectives on nuclear disarmament in light of the contradictory strategies of nuclear powers]. *Međunarodna politika, 63*(1145), pp. 110–126. Downloaded 2025, January 10 from: http://repozitorijum.diplomacy.bg.ac.rs/123/1/Medjunarodna%20politika%201145-2012-112-128.pdf
25. The Treaty for the Prohibition of Nuclear Weapons in Latin America and the Caribbean. Downloaded 2025, January 10 from: https://treaties.un.org/doc/Publication/UNTS/Volume%20634/volume-634-I-9068-English.pdf
26. The Treaty on the non-proliferation of nuclear weapons. Downloaded 2025, January 10 from: https://www.iaea.org/sites/default/files/publications/documents/infcircs/1970/infcirc140.pdf
27. Urwin, J. A. (2016). More bang for your buck: Nuclear weapons and their enactment of colonial and gendered power. *The ANU Undergraduate Research Journal, 8*, pp. 237–250. DOI: 10.22459/AURJ.08.2016.18.
28. Vukadinović, R. (2006). Nuklearno oružje u posthladnoratovskom svijetu [Nuclear weapons in the Post-Cold War World]. *Međunarodne studije, 6*(3), pp. 130–140. Downloaded 2025, January 10 from: https://hrcak.srce.hr/file/421383
29. Williams, P. (2011). *Race, ethnicity and nuclear war: Representations of nuclear weapons and post-apocalyptic worlds*. Liverpool: Liverpool University Press
30. Žirovčić, D. (2009). Bliskoistočna nuklearna enigma [The Middle Eastern nuclear enigma]. *Međunarodne studije, 9*(4), pp. 90–103. Downloaded 2025, January 10 from: https://hrcak.srce.hr/file/421849

Kovačević Anika*
https://orcid.org/0000-0002-5632-1917
Milosavljević Nikola**
https://orcid.org/0000-0003-0208-2807

UDK: 342.7:347.78
Review article
DOI: 10.5937/ptp2502075K
Received on: March 10, 2025
Approved for publication on:
May 5, 2025
Pages: 75–89

THE RIGHT OF DIVULGATION AS A FORM OF THE RIGHT TO PRIVACY

ABSTRACT: The author's personal right of divulgation—the right to publish a work—is not universally recognized in all countries. Considering its potential significance for the author, it is necessary to examine the rationale behind its legal regulation. To that end, in the first part of the paper, the authors, applying legal dogmatic and sociological methods, analyze the right to privacy, its legal foundations, and its various forms. In the second part, using the legal dogmatic method, they examine the concept and scope of the right of divulgation and conduct a comparative legal analysis. By applying deductive and comparative methods, the authors further explore potential legal grounds for the recognition of the right of divulgation, particularly its relationship with the right to privacy. Based on this analysis, the authors conclude that the right of divulgation can be viewed as a form of the right to privacy, thereby highlighting the need for its broader international recognition in order to protect the author's privacy interests.

Keywords: *right to privacy, human rights, constitutional rights, right of divulgation, protection of author's privacy, author's moral rights.*

* LLD, Assistant Professor, University of Kragujevac, Faculty of Law, Kragujevac, Serbia, e-mail: akovacevic@jura.kg.ac.rs
** LLD, Assistant Professor, University of Kragujevac, Faculty of Law, Kragujevac, Serbia e-mail: nmilosavljevic@jura.kg.ac.rs

1. Introduction

Legal positivism declares that each legal norm has its roots in the legal norm of higher legal power. This premise is quite important when we discuss human rights. It is possible to argue actually that every right that is recognized in regulations can be derived from the rights that are enumerated in a constitutional bill of rights or international convention that provides that right. This brings us slowly to the problem of copyright. In most texts, the copyright is usually derived from the constitutional or conventional guarantee of the author's rights concerning his/her work of authorship. However, this guarantee in most constitutions is limited to recognition of the economic rights that the author has, meaning that his/her right to exploit his/her work shall not be violated. Yet in a number of countries, including the Republic of Serbia, moral rights are also recognized to the author and not just economic rights. It is quite challenging to try to derive moral rights from the constitutional or conventional guarantee of copyright since it is mostly concerned with the author's right to bear fruits from his/her work. In this paper, we will analyze one of the author's moral rights – the right of divulgation and try to trace its source back to the right to privacy. In order to prove our thesis, we divided the research into two parts. In the first part, we analyze the right to privacy. We examined the legal basis and development of this right in order to conclude how firmly recognized this right is worldwide. After that, we will try to show that the right to privacy, somewhat more than other human rights, can be recognized in many different manifestations. In the second part of our research, we first examine the definition of the right of divulgation, as well as its comparative recognition. At the end, we will discuss possible sources of the right of divulgation, and examine its connection to the right to privacy.

2. The Concept of the right to privacy

The right to privacy is one of the basic, inalienable and absolute human rights of every individual, which ensures the integrity and dignity of humans, and in order to preserve the secrecy and freedom of their private lives. The right to privacy protects three types of interests: a) a person's interest in the autonomy of decision-making in intimate and personal matters; b) the interest of the individual to protect himself/herself from disclosure of personal circumstances; c) the individual's interest to be protected from unfounded surveillance by the authorities (Dimitrijević, 2011, p. 202) and other data collections. sector, often for commercial purposes.

Therefore, in the matter of international human rights, we observe the relationship between the state and the individual, and such behavior in relation to the individual as practically the behavior of the state itself, according to the standard model of the manifestation of the state (by branches of government, and the behavior of civil servants within their jurisdiction, etc. according to the rules on responsibility of the state). The idea of privacy, as well as the legal formulations presented in the form of the history of the right to privacy, are still the same today. Two characteristics of today's global society fundamentally affect the understanding and application of the right to privacy – (1) the speed and availability of information, and especially electronic information, and (2) the degree of endangerment of both individuals and states by misuse of information (Rengel, 2013, pp. 32–34). While in the earlier phase of the development of the right to privacy it was perceived that the states that threatened this right are authoritarian and totalitarian, today there is a pronounced tendency to limit or deny the right to privacy also by highly developed democratic, liberal states by referring to the principle of national security.

Publication of information that violates honor, reputation or piety, i.e. it shows the face in a false light by attributing features or properties that it does not have, that is by renouncing the features or properties it has, is not allowed under provided that the interest in publishing information "of this kind information" does not outweigh the interest to protect dignity and the right to authenticity, especially if the publication does not contribute public discussion about the specific phenomenon, event or person in question (Vučković, 2023, p. 225).

Here, we point to the concept of public, which is opposite to the concept of privacy. We can understand the public as a sphere of social life in which the emergence and networking of various private and social interests, activities and needs that are known or available to all persons or to the majority occurs (Andonović, 2019). The right to privacy is strictly a personal right, as its enjoyment and use cannot be transferred to another. It is broad, encompassing various aspects of an individual's personality and personal assets, which is why it is often subdivided into more specific rights in both regulations and theory (Logarušić & Lazić, 2023). Over time, privacy has become an increasingly important personal good and a key focus in legal theory and practice.

3. Review on international documents thtat regulate right to privacy

3.1. The right to privacy in the Universal Declaration of Human Rights

On the subject of the right to privacy, we emphasize the importance of, we can say, the founding document on human rights – the Universal Declaration of Human Rights from 1948. (Universal Declaration of Human Rights, 1948) The right to privacy is recognized in the preamble itself, which states the reasons for adopting the Declaration. Then, the Right to Privacy is explicitly stipulated in Article 12 of the Declaration: "No one shall be subjected to arbitrary interference with his/her privacy, family, home or correspondence, nor to attacks upon his/her honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" (Universal Declaration of Human Rights, 1948, art. 12). However, the Declaration does not guarantee complete freedom from interference in private life, but only freedom from "arbitrary interference", and accordingly, this standard allows for different interpretations. Please note that this document is of a declarative nature and that its basic purpose and goal is to universally promote the most important human rights and freedoms.

3.2. The right to privacy in the International Covenant on Civil and Political Rights

The right to privacy is provided for in the International Covenant on Civil and Political Rights from 1976 (International Covenant on Civil and Political Rights, 1976). This document protects the basic civil and political rights of individuals. The Covenant contains the same provision on the right to privacy as the Universal Declaration of Human Rights. It is stipulated that no one can be exposed to arbitrary or illegal interference in private life, family, apartment or correspondence, nor to illegal attacks on honor and reputation (International Covenant on Civil and Political Rights, 1976, art. 17).

According to the provisions of the Covenant, in its basic setting, the right to privacy is consistent. It consists of the right to private life, the right to respect an individual's family life, the right to respect home and the right to conduct correspondence – communication. All these individual rights additionally branch out into a number of forms. The normative classification of the right to privacy is not the only one. In addition to this classification, a number of other theoretical classifications appear based on different criteria

or aspects of people's lives (Boban, 2012, pp. 575–576). In that manner, for example, we can talk about the protection of the privacy of personal data, the right to the privacy of the body and organism (in the sense of the exclusive and independent decision to undergo medical tests for drugs, AIDS, alcohol, etc.), the right to the privacy of communications, the privacy of the environment. It was precisely on one of the above-mentioned isolated fragments that the Council of Europe convention was created – the Convention on Privacy, as it is popularly called, i.e. Council of Europe Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data from 1981 (Convention on Automatic Processing of Personal Data, 1981). To date, 41 countries have ratified this Convention, Serbia in 2005 (entered into force in 2006). The subject of the Convention is the harmonization of the national legislation of the signatory states with the basic principles and recommendations contained in this document. Respecting the rule of law, human rights and basic freedoms, the Convention aims to connect its members, expand the protection of basic rights and freedoms of the individual, especially the right to privacy, when it comes to the automatic processing of personal data. States are left with the initiative to decide on the content and scope of personal data protection in the process of regulating this matter, with the possibility of expressing and preserving certain specificities. At the same time, each country must adhere to established principles.

3.3. The right to privacy in the European Convention on the Protection of Human Rights and Fundamental Freedoms

In 1950, the European Council adopted the European Convention on the Protection of Human Rights and Fundamental Freedoms, which in Article 8 recognizes the right to privacy as the right to private and family life: "1) Everyone has the right to have respect of his/her private and family life, home and correspondence; 2) The public authority will not interfere in the exercise of that right, except in accordance with the law and if in a democratic society it is necessary in the interest of national security, public order and peace, or the welfare of the country and for the prevention of disorder or crime, for the protection of health or morals, or in order to protect the rights and freedoms of others" (Convention for the Protection of Human Rights and Fundamental Freedoms, 1950). Although the provisions of the convention itself do not elaborate in detail the issue of individual privacy protection and that rather broad exceptions to the protection of rights are listed, it is obvious that "the convention tried to encompass the general right to individual privacy as one

of basic human rights" (Klarić, 2016, p. 989). The right to privacy, therefore, guaranteed by Article 8 of the European Convention on Human Rights, allows a person not only to be protected from interference by the authorities but also from interference by other individuals and institutions, including the means of mass communication. The term "respect" covers the protection of the individual against self-willed interference by public authorities regarding his/her privacy, but also obliges the state to actively participate in ensuring this right.[1]

4. The right of Divulgation

4.1. The definition and the regulatory framework of the Right of Divulgation

Moral rights of the author represent a group of legal rights that are not globally accepted. Among moral rights, the right of divulgation (right of disclosure, right of publication, right of dissemination) is recognized as even more controversial. In fact, the right was so controversial that it was not included in the Berne convention because of this (Kwall, 1985, p. 804). Nonetheless, some believe that this right is implicitly recognized in the Berne Convention through provisions about publication (Radakova, 2001, pp. 69–70). It was not accepted by the common law countries, but it was also not recognized among all continental countries either. USA does not provide this right, although it introduced some of moral rights both on state and federation level (paternity right and right of integrity), and neither does UK. However, there were instances in which English Courts awarded protection for the right of divulgation under common law. In *Pope vs. Curl*, case from 1741, Lord Chancellor Hardwicke founded the right of disclosure by recognizing that a publisher cannot disclose work of authorship without the consent of the author since he treated work as joint property of author and publisher (Sirvinskaite, 2010, p. 272). The Canadian legislature to this day stands on this opinion and does not recognize right of divulgation as such, although it treat it as implied by economic rights (Adusei, 2007/2008, p. 4). On the other hand, Germany, for instance, didn't specifically recognize this right as such until 1965, because it was believed that it was implied by other economic rights of the author (Marković, 1999, p. 177). The country that was the

[1] Report of the European Commission 79/267/EEC of 11. March 1979, par. 52; cited according to (Dimitrijević & Paunović, 1997, p. 286).

cradle of this right is France. It is recognized in Switzerland, Spain, and Italy as well (Radakova, 2001, p. 68). This right was developed from the court cases. There were a few cases where French courts awarded protection to the author's right to disclose his/her work of authorship: *Murate c. Neville* from 1546, *Marle c. Lacordaie* and *Marquam c. Lehuby*, both from 1845 (Sirvinskaite, 2010, pp. 275–276), or *Whistler v. Eden* from 1900 (Omondi, 2019, p. 13). In the case of the *Cour d'appell* in Paris, *Carco v Camoin* from 1931, the French court held that only the author of the work can decide if and when the work is finished, and therefore whether it should be presented to the public (Hansmann & Santilli, 1997, pp. 136–137). Many definitions of this right were built upon the *Carco v Camoin* case. According to them right of divulgation is right of the author to decide if the work of authorship is finished and worth showing to the public (Kwall, 1985, p. 5; Hansmann & Santilli, 1997, p. 136; Lee, 2001, pp. 801–802). Other theoreticians emphasize the importance of the moment of publication for the author and therefore regard this right as the right of "publication management". In their opinion, the right of divulgation enables the author to decide whether should work of authorship be published, as well as where, how, and when it shall be published (Pink, 1994, p. 174). For some, it is right of the author to deny publication of the work of authorship regardless of his/her contractual obligations and the fact that s/he already transferred his/her economic rights. Therefore, it represents an unnecessary burden (Radakova, 2001, pp. 69–71; Hansmann & Santilli, 1997, p. 139; Gibbens, 1989, pp. 455–456). There are different definitions in the legislature as well. According to the French Code of intellectual property, only the author is authorized to divulge his/her work of authorship, and it is only s/he who defines the procedure and conditions for publication (Code de la propriété intellectuelle, sec. L-121-2). German Act on Copyright and related rights stipulates that the author has the right to determine whether and how his/her work is to be published (Urheberrechtsgesetz, sec. 12.). The right of divulgation is recognized in the Serbian Law on Copyright and related rights as well, so it is provided that only the author has the right to publish his/her work of authorship and to decide how it will be published (Law on Copyright and related right, 2009, sec. 16. par. 1).

Right of divulgation means that only the author is to decide if the work of authorship is finished or not. Only the author can say if his/her work is perfected, since only s/he can tell if it is what s/he imagined. Publishing work that is of no quality or lower quality than usual could severely damage the author's reputation. Moreover, it could be possible that the author has finished the work and that s/he is satisfied with it, but s/he waits the right moment to

present it to the public. The timing of publication could influence the success of the work of authorship greatly. In Serbian and German law (Law on Copyright and related right, 2009 sec. 16 par. 2; Urheberrechtsgesetz, 1965, sec. 12 par. (2)) the author also exclusively has the right to give information or describe his/her work. This also stands for Hungarian law (Sápi, 2020, p. 119). That represents a natural extension, and it is also important for the management of the publication since there is a necessity to announce the work before it is published. This, of course, is important only when an author gives out the original elements of his/her work of authorship, since otherwise this would not represent the divulgation of the work (Marković, 1999, p. 176). The author can only once disclose to the public his/her work. However, if anyone discloses an author's work without his/her permission, there is legal fiction that the disclosure hasn't occurred (Sápi, 2020, p. 156). The restrictions of copyright (fair use doctrine) cannot be used if the work of authorship is not disclosed. This stands for Serbian law, as well as for most continental jurisdictions, but it is not universally accepted, nor do all countries provide it in the same manner. For instance, German law provides that it is necessary for work of authorship to be disclosed in order to use restrictions of the copyright, with the exception of the limitation for using work in court or administrative proceedings (Omondi, 2019, p. 95). Therefore, if the author didn't disclose his/her work, no one can use it without his/her permission (Marković, 1999, p. 223). The restrictions are provided in cases when some interest is more important than the property interest of the author (public necessity, education, public information, etc.). This basically means that the legal system gives more importance to the right of divulgation than the other interests. In addition, it is provided that even when the author transfers his/her economic rights through contract, it cannot be considered that s/he implicitly agreed to divulge his/her work in such manner. It is necessary that the author explicitly allowed divulgation of the work in contract (Law on Copyright and related rights, sec. 68. par. 2.). However, Japanese legislation, for instance, has the opposite solution: if the copyright was transferred to the contractual party it will be implied that author allowed divulgation (Zhang, 2012, p. 37). This stands for Hungarian law as well (Sápi, 2020, p. 119). Besides, the original work of authorship cannot be judicially sized in execution proceedings (Law on civil enforcement, 2015, sec. 218. par. 1. lin. 4)), which means that the right of divulgation supersedes the pecuniary interests of the third party. This is recognized even in the USA, which does not provide the right of divulgation explicitly (Zhang, 2012, p. 11). Finally, the author can perform this right even after his/her death. On the one hand, there are theoreticians who claim that the

work of authorship cannot be disclosed after the author's death unless it was his/her wish. On the other hand there are theoreticians that claim that work can be disclosed unless the author openly forbade it while s/he was alive. This solution is accepted in Serbian law (Ivanović, 2012, p. 61). In both cases author has control over disclosure of his/her work, and, unless s/he wanted, it will not become available to the public.[2]

4.2. The justification and the possible source of the right of divulgation

There are many explanations on why an author should have the exclusive right to decide if the work of authorship should be disclosed or not. First of all, there is the theory of natural rights. Namely, as God created the Universe s/he is his/her sole master, so the author is the master of his/her work s/he created. It is his/her "natural", "divine" right to make all of the decisions concerning the destiny of his/her work, including divulgation (Sirvinskaite, 2010, p. 276). There are theories that emphasize the author's personality as a key point of protection. Under these opinions that derive from Hegel's and Kant's philosophy, the work of authorship represents the author's personality that has been externalized (Omondi, 2019, p. 18). The author has sole discretion to decide in what manner s/he will present and unveil his/her personhood expressed in his/her work (Zhang, 2012, p. 10). Every attack on work of authorship is an attack on the author's personality, and an author has the right to prevent such an attack and criticism (Davis, 1985, p. 246). Similar opinions state that the work of authorship represents an externalized "social self", meaning that the work of authorship is not just personality *per se*, but the author's personality as perceived by others. Right of divulgation in that system should represent the power of the author to decide whether there should be an externalized "social self" and in which particular manner does author wants to represent his/her "social self" to the public (Simon, 2023, pp. 20–26). Other opinions stipulate that the main protection object is the author's professional reputation (Zhang, 2012, p. 15). The author discloses works of authorship of certain quality, therefore it is expected of him/her not to create work that is not as good as his/her previous works (Kwall, 1985, p. 25). Similar to these opinions are the theories that perceive the right of divulgation as the right of impression management. It determines the moment when the work enters the financial and commercial sphere (Simon, 2023, p.

[2] In French and Bosnian law, there is a limited group of heirs that can perform divulgation after the death of the author (Kwall, 1985, p. 16; Omondi, 2019, p. 76; Ivanović, 2012, p. 56).

34). Author, as a person who is most interested in the success of work, has the right to decide if, when, where and how the work will be disclosed to the public (Kwall, 1985, p. 87).

In the Serbian theory, there is a discussion about the treatment of moral rights. For some theoreticians, the moral rights of the author represent a form of rights of personality. Others believe that there are no similarities between moral rights and rights of personality because rights of personality are directly protecting personality (his physical and moral integrity), while moral rights of the author protect the work of authorship, which is not technically part of the author's personality, so they protect it indirectly (Dudaš, 2006, pp. 269–270, Ivanović, 2012, p. 51). Rights of personality protect "person-citizen", while moral rights protect specific "person-creator". Moral rights represent instruments for protecting the permanent connection that emerges between the author and his/her work. They are a specific form of rights of personality that is adopted for human creativity. Hence, there is a difference between civil rights protected by constitutional law, and rights of personality protected in civil proceedings. Moral rights of the author are the form of rights of personality but not a civil rights protected by constitutional law (Radojković, 1964, p. 265). In our opinion, it is wrong to make such a sharp division between the rights of personality and civil rights, since ultimately, all rights could be derived from civil rights. If we analyze the different forms and boundaries of the right of divulgation, we could easily realize that the right of divulgation is not a right to disclose work but rather a right not to disclose a work. The way in which boundaries were set clearly implies that their purpose is to protect author's privacy. Most authors create in order to be famous and accepted. Nevertheless the author's work represents the materialization of his/her thoughts, and thoughts represent the author's private area. Any different solution would suggest that an author has to publish his/her thoughts if s/he obliged by contract or law. The main point of protection here is not reputation *per se* but the dignity of the author. Public disclosure of the author's work degrades him/her as a person, leaving his/her life open to public. This does not represent defamation, but an insult to individuality (Bloustein, 1964, p. 981). It could be possible that the author created masterpiece by all standards, and publication of such work does not do any harm to his/her reputation, even the opposite. Yet it is only his/her decision if that part of his/her privacy should be shared with other people, since it is possible that s/he created work about things s/he would not share. In this matter, a work of authorship is no different from a diary or a letter (Warren & Brandais, 1980, p. 70). Sole act of disclosure could be embarrassing, whether the work was good or not. Emotions and thoughts

communicated through a work of art could represent the darkest place of an author's mind, and it would be against human nature to make someone share it, since it would represent an invasion of privacy (Kwall, 1985, p. 26). An author would be "…less of a man, less of a master over his/her own destiny, were s/he without this right" (Bloustein, 1964, p. 971). Therefore, we agree with the opinion that the right of divulgation is an enforcement of the right to be left alone (Warren & Brandais, 1980, pp. 73–74).

There are practical implications of this theoretical consideration. First of all, it makes it possible to protect the right of divulgation through the right of privacy under article 8 of European Charterer of Human Rights. Further, in jurisdictions that don't recognize this right, it could be protected indirectly through the right of privacy or right of private communication, which is the case, for instance, in the USA. Finally, when performing the proportionality test, there would be a different treatment of this right if it is known that it is derived from the right to privacy. Therefore, we strongly believe that the correlation between the right to privacy and the right of divulgation has a firm foundation, and that most authors would benefit from this correlation.

5. Concluding remarks

From the conducted research, we derived the following conclusions. First of all right to privacy is a universally recognized human right, contained in most of the constitutions and international conventions. We could also conclude that the right to privacy has many manifestations. On the other hand, the right of divulgation is a moral right of the author, not universally recognized, in fact recognized by very few countries. It enables the author to choose whether or not to share his/her work of authorship publicly. This right is quite necessary for the author. As research has shown, the right of divulgation is principally important for the protection of the author's privacy. As well as with personal correspondence, the author's thoughts are the very last private shelter in this ultra-publicly available society. Not all authors want that part of their personality to become public, so that decision should be respected. We have seen that the right to privacy has the very same purpose – to prevent parts of a person's personality from becoming public. Hence, the relationship between these two rights is a general-specific relationship. We therefore believe that the main hypothesis of this work – that the right of divulgation can be derived from the right to privacy is confirmed. Therefore, it is safe to assume that the right of divulgation is a specific form of right to privacy that protects privacy in creativity as an aspect of human nature.

Kovačević Anika
Univerzitet u Kragujevcu, Pravni fakultet, Kragujevac, Srbija

Milosavljević Nikola
Univerzitet u Kragujevcu, Pravni fakultet, Kragujevac, Srbija

PRAVO NA OBJAVLJIVANJE KAO OBLIK PRAVA NA PRIVATNOST

APSTRAKT: Ličnopravno ovlašćenje autora na objavljivanje autorskog dela nije univerzalno priznato u svim državama sveta. Imajući u vidu njegov potencijalni značaj za autora, potrebno je ispitati šta je razlog njegovog propisivanja. U tom cilju autori u prvom delu, rada primenom pravnodogmatskog i sociološkog metoda, analiziraju pravo na privatnost, njegovu definiciju pravne osnove i pojavne oblike. U drugom delu rada autori primenom pravnodogmatskog metoda ispituju pojam prava na objavljivanje, kao i granice njegove primene i sprovode uporednopravnu analizu prava na objavljivanje. Primenom deduktivnog i komparativnog metoda autori na kraju ispituju moguće osnove za priznanje prava na objavljivanje i posebno odnos sa pravom na privatnost. Sprovedenom analizom autori utvrđuju da se pravo na objavljivanje može smatrati oblikom prava na privatnost, te otuda postoji potreba za njegovim širim priznavanjem u svetu u cilju zaštite interesa privatnosti autora.

Ključne reči: *pravo na privatnost, ljudska prava, ustavna prava, pravo na objavljivanje autorskog dela, zaštita privatnosti autora, ličnopravna ovlašćenja autora.*

References

1. Adusei, P. (2007/2008). 21st Century Protection of Moral Rights under Copyright Law: The Way Forward. *KNUST Law Journal*, pp. *4*(1), pp. 1–19
2. Andonović, S. (2019). *Zaštita podatka u elektronskoj javnoj upravi u Republici Srbiji* [*The Personal Data Protection in Digital Public Administration*]. Beograd: Pravni fakultet Univerzitet u Beogradu

3. Bjelajac, Ž., & Filipović, A. (2021). Specific characteristics of digital violence and digital crime. *Pravo – teorija i praksa, 38*(4), pp. 16–32
4. Bloustein, E. J. (1964). Privacy as an aspect of human dignity: an answer to dean Prosser. *New York University Law Review, 39*(6), pp. 962–1007
5. Boban, M. (2012). Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom društvu [The Right to Privacy and the Right to Access Information in the Modern Information Society]. *Zbornik radova Pravnog fakulteta u Splitu*, *49*(3), pp. 575–598.
6. Code de la propriété intellectuelle, loi no 92-597 du 1er juillet 1992 [*French Intellectual property Code*]. (n.d.)
7. Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14, CETS 005 of 4. December 1950. (1950)
8. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, ETS 108 of 28. January 1981. (1981).
9. Davis, S. (1985). State moral rights law and the federal copyright system. *Cardozo Arts & Entertainment Law Journal, 4*(2), pp. 233–260
10. Dimitrijević, P. (2011). Pravna regulacija elektronske komunikacije i pravo na privatnost [Legal Regulation of Electronic Communication and Right on Privacy]. In: Marković, R. (ured.), *Zbornik radova Pravnog fakulteta Univerziteta u Istočnom Sarajevu* [*Proceedings of the Faculty of Law, University of East Sarajevo.*] (pp. 199–211). Istočno Sarajevo: Pravni fakultet u Istočnom Sarajevu
11. Dimitrijević, V., & Paunović, M. (1997). *Ljudska prava* [*Human Rights*]. Beograd: Beogradski centar za ljudska prava
12. Dudaš, A. (2006). Naknada štete zbog povrede ličnih prava autora[Civil Actions for the Protection of Author's Moral Rights]. *Zbornik radova Pravnog fakulteta u Novom Sadu, 40*(2), pp. 263–288
13. Gibbens, R. D. (1989). The Moral Rights of Artists and the Copyright Act Amendments. *Canadian Business Law Journal, 15*(4), pp. 441–470
14. Gutić, S. (2010). Pravo na privatnost u Evropskoj konvenciji za zaštitu ljudskih prava i osnovnih sloboda [The Right to Privacy in European Convention on Human Rights]. *Strani pravni život, 54*(2), pp. 335–346
15. Hansmann, H., & Santilli, M. (1997). Authors' and Artists' Moral Rights: A Comparative Legal and Economic Analysis. *The Journal of Legal Studies, 26*(1), pp. 95–144

16. Human Rights Committee. (1988). *Report of the Human Rights Committee, Supplement (A/43/40), Annex VI,* General Comment 16 (32) d (28 September 1988)
17. International Covenant on Civil and Political Rights 2200A, Un doc. S/ RES 2200A,. (1976)
18. Ivanović, S. (2012). Nasljeđivanje subjektivnog autorskog prava [Inheritance of Copyright]. *Godišnjak Pravnog fakulteta*, *3*(2), pp. 43–66
19. Jakšić, A. (2006). *European Convention on Human Rights – Commentary.* Belgrade: Faculty of Law University of Belgrade
20. Klarić, M. (2016). Zaštita osobnih podataka i Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda [Protection of Personal Data and "ECHR"]. *Zbornik radova Pravnog Fakulteta u Splitu*, *53*(4), pp. 973–990
21. Kwall, R. R. (1985). Copyright and the Moral Right: is an American Marriage Possible. *Vanderbilt Law Review, 38*(1), pp. 1–100
22. Lee, I. (2001). Toward an American Moral Rights in Copyright. *Washington and Lee Law Review, 58*(3), pp. 795–854
23. Lloyd, I. J. (1985). The Data Protection Act – Little Brother fights back? *The Modern Law Review, 48*(2), pp. 190–200
24. Logarušić, D., & Lazić, I. (2023). Personal rights and freedoms – the forms and trend of protection. *Pravo – teorija i praksa, 40*(1), pp. 1-12
25. Marković, S. (1999). *Autorsko i srodna prava* [*Copyright and Related rights*]. Beograd: Službeni glasnik
26. Omondi, O. B. (2019). *The Right of Divulgation: Expanding the Scope of Authors' Moral Rights under the Copyright Act 2001.* Eldoret: MOI University
27. Pink, J. S. (1994). Moral Rights: Copyright Conflict between the United States and Canada. *Southwestern Journal of Law and Trade in the Americas, 1*, pp. 171–196
28. Radakova, L. (2001). *Moral Rights of Authors in International Copyright of the 21st Century: Time for Consolidation – master thesis.* Vancouver: University of British Columbia
29. Radojković, Ž. (1964). Prava ličnosti i njihov odnos prema ličnopravnim (moralnim) elementima autorskog prava [The rights of personality and their connection to the moral elements of copyright]. *Anali Pravnog fakulteta Univerziteta u Beogradu, 12*(2-3), pp. 263–279
30. Rengel, A. (2013). *Privacy in the 21st Century.* Leiden, Boston: Martinus Nijhoff Publishers.
31. Report of the European Commission 79/267/EEC of 11. March 1979

32. Rubenfeld, J. (1989). The right of privacy. *Harvard Law Review, 102*(4), pp. 737–807
33. Sápi, E. (2020). Moral Rights of Authors – an Overview with Special Regard to the Right to Integrity. In: Csak, C. E. (eds.), *Modern Researches: Progress of the Legislation of Ukraine and Experience of the European Union* (pp. 117–134). Miskolc: University of Miskolc
34. Schoeman, F. D. (1984). *Philosophical Dimensions of Privacy: An Anthology.* Cambridge: Cambridge University Press
35. Simon, D. A. (2023). Copyright, Moral Rights, and the Social Self. *Yale Journal of Law & the Humanities, 34*(4), pp. 263–288
36. Sirvinskaite, I. (2010). Toward Copyright Europeanification: European Union Moral Rights. *Journal of International Media & Entertainment Law, 3*(2), pp. 263–288
37. Šurlan, T. (2014). Međunarodnopravna zaštita prava na privatnost [Right to Privacy – International Law Normative Framework]. *Srpska pravna misao, 20*(47), pp. 47–73
38. *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights E/CN. 4.,* Un doc. S/RES/4/1985 (28. September 1985). (1985)
39. *Universal Declaration of Human Rights,* Un doc. S/RES/217A (10 December 1948). (1948).
40. United Nations General Assembly. (2014). *The right to privacy in the digital age,* A/HRC/27/37
41. *Urheberrechtsgesetz German copyright law* vom 9. September 1965 (BGBl. I S. 1273), das zuletzt durch Artikel 25 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858) geändert worden ist. (n.d.).
42. Vučković, J. (2023). *Mediji i medijsko pravo* [*Media and media law*] Kragujevac: Pravni fakultet Univerziteta u Kragujevcu; Institut za pravne i društvene nauke
43. Warren, S. D., & Brandais, L. D. (1980). The Right to Privacy. *Harvard Law Review, 4*(5), pp. 193–220
44. Zakon o autorskom i srodnim pravima [Law on Copyright and neighboring rights]. *Službeni glasnik RS,* br. 104/09, 99/11, 119/12, 29/2016 i 66/19
45. Zakon o izvršenju i obezbeđenju [Law on civil enforcement*]. Službeni glasnik RS,* br. 106/15, 106/16, 113/17, 54/19, 9/20 i 10/23
46. Zhang, J. (2012). *Restrictions on Moral Rights – A Comparative Study on Its Legislation and Application in Civil Law and Common Law Jurisdictions – master thesis.* Toronto: University of Toronto

Logarušić Dejan[*]
https://orcid.org/0000-0001-9782-9277
Rapajić Milan[**]
https://orcid.org/0000-0002-1268-6826

UDK: 340.12:340.131
Review article
DOI: 10.5937/ptp2502090L
Received on: April 22, 2025
Approved for publication on:
May 9, 2025
Pages: 90–101

THE SIGNIFICANCE AND CONNECTION OF THE PRINCIPLES OF CONSTITUTIONALITY AND LEGALITY WITH THE LEGAL ORDER AND RULE OF LAW

ABSTRACT: The rule of law is one of the oldest and most significant ideas in the history of legal and political thought. Contemporary legal scholars widely emphasize that this concept occupies a central place in clearly articulated views concerning the state, law, politics, and economics. As an ideal worth striving toward, the rule of law has been addressed by leading figures in law, economics, and political theory.

The discourse on the principles of constitutionality and legality has consistently served as a cornerstone in affirming the importance of the rule of law in modern legal systems. This is particularly relevant given that these principles are essential to the existence of the legal state. In accordance with the focus of this paper, the authors analyze several key issues: how to determine the significance of the relationship between the principles of constitutionality and legality and the rule of law, how to conceptually present the essence of constitutionality, legality, the rule of law, and the legal state.

.

[*] LLD, Associate Professor, Faculty of Law for Commerce and Judiciary in Novi Sad, University Business Academy in Novi Sad, Novi Sad, Serbia, e-mail: dejan.logarusic@pravni-fakultet.info

[**] LLD, Associate Professor, Faculty of Law, University of Kragujevac, Kragujevac, Serbia, e-mail: mrapajic@jura.kg.ac.rs

Keywords: *rule of law, legal state, constitutionality, legality, legal theory.*

1. Introduction

The rule of law, as an idea, is one of the oldest and the most important ideas in the history of legal and political thought.

The first ideas about a legal state and the rule of law and laws find their origin in "the deep past of legal and political thought. Greek philosophy represented fertile ground for the development of certain elements of these models" (Avramović, 2010, p. 424). Namely, Greek political and legal thought was initially on the stand that "the rule of law is not the rule of any law, but the laws which have been created by the men of thought whose goal was to achieve virtue and general good and well-being and freedom of the citizens in Greek polis" (Tadić, 1996, p. 23).

Later on, the legal thought in ancient Rome relied on Greek experience, based on the ideas of Plato, Solon, Perikles and Aristotle, which through the evolution of legal and political thought emphasized that the laws are necessary and more important than the rule of thought of distinguished wise men (for more, see: Čavoški, 1994, p. 16). In support of this opinion, Avramović (2010) pointed out that "in ancient Rome, Cicero came nearest to the idea of legal state and rule of law. According to him, the existance of good laws represented the guarantee of a good state order" (p. 424).

In the theory of new age, "human rights are viewed as natural, legally based rights of every human being. The mere purpose of a political community, within the scope of liberal thought, is essentially different from the one existing in ancient Greece and Rome; now the state needs to provide the protection of individual rights and set the boundaries that the members of community, including the members of ruling class, may not cross in their conduct and not only to worry about the virtue and moral of its citizens, as it was the case in ancient times. The idea of freedom, within the scope of liberal thought, is defined as freedom to act without causing damage to other people, with a clearly defined requirement that the boundaries for individual conduct must be set by law as a source of rules which regulates necessary rectrictions of individul freedom" (Zekavica, 2018, p. 13). Hence, we can underline that the idea of the rule of law also lies in the restriction of state power by its own laws and that it is not enough just to have a normative framework in order to fully apply the concept of the rule of law. Namely the existence of laws is the vital requirement for the realization of the idea of the rule of law, but in addition to a well established normative framework, it is imporatnt that it is

fully applied and that this application is substantive and value-based. In other words, "legal norms exist so that people can behave in compliance with them. Legal system functions well if the subjects, to whom these norms are directed, comply with them" (Kulić & Kulić, 2015, p. 167). This normative framework should reflect the importance of interconnection between the rule of law and the principles of constitutionality and legality in one state.

In this paper the authors, in the context of the headline theme, will discuss a few important questions – how to define the significance of mutual concord and connection, between the principles of constitutionality and legality and the rule of law, as well as between the rule of law and legal state and how to present the conceptual essence of constitutionality.

2. The significance of mutual concord and connection between the principles of constitutionality and legality and the rule of law

In legal theory, first there was an assumption that "law in external world was manifested as a set of rules of conduct prescribed by the dominant form of social organization (state)" (Mandić, 2017, p. 9). Legal theorists which support this stand are called normativists who, accordingly, "consider that lawfulness, as the key determinant of legal rules, can only be viewed as factual compliance with the rules of conduct prescribed the legal order and expressed though the disposition of legal norm" (Carbonnier, 1992, p. 141). However, a number of authors believe that law "should not be viewed as a set of norms, but as the actual conduct of people. The essence of their theory is that the existence of legal norms which regulate how individuals should behave is not what is important for the concept of law. According to them, what only matters is how people really behave in their everyday lives. Consequently, they believe that law is not a normative, but rather a factual science whose goal is to study human behavior and to norm it up" (Mandić, 2017, p. 9; also see: Kelzen, 1951, p. 64).

When analyzing different approaches in determining law and legal order, the authors also have noted the opinion according to which "law, before all, represents the order of subjects and their immanent law-making sources based on which, accordingly, a legal norm represents one of many elements of legal order" (Prica, 2018, p. 104). The authors also underline that "for the thought of a concrete legal order, "the order" does not mean a rule, or a set of rules, but, on the contrary, the rule is only its constituent part and a tool used by that order. Accordingly, the thought of norms and the thought of rules represent

just one part, the restricted and derived element, of comprehensive legal and scientific task and work" (Schmitt, 2003, p. 9).

Generally, legal order is based on the hierarchy of legal norms. Accordingly, "lower legal acts and material acts of human conduct, connected with the application of legal norms, i.e. to the conduct complying with the legal norms which are the part of these legal acts, must be in accord with the constitution and laws, as the supreme legal acts. It is of vital significance that all segments of legal order are mutually harmonized, since only when they are in a complete concord they can achieve desired goals" (Kulić & Kulić, 2015, p. 168). The authors often underline the importance and need that the conduct of the members of community should be in accord with the requirements prescribed by legal norms and that the legal acts of lower legal force must be in agreement with the legal acts of superior power. In this way we will obtain "the unity of legal order where conditions are created for efficient protection and successful realization of social values proclaimed by them. These values are connected with justice, freedom, human dignity, tolerance, etc." (Kulić & Kulić, 2015, p. 168).

However, the principle of the rule of law and legal state receives its full meaning in contemporary society and it is one of the most important heritage of civilization. The principle of the rule of law and legal state actually means that all citizens, institutions, and organizations, including the government bodies, are accountable to the legal order. The constitution and laws define the rules of conduct which are binding for all people. Here we should emphasize that according to the principle of the rule of law and legal state no power is above law and all citizens are equal before law.

As it is often pointed out in theory, in relation to the discourse on mutual concord and connection between the principle of constitutionality and legality and the rule of law, "the principle of constitutionality and legality is closely related to the rule of law and legal state. Without the application of this principle, the rule of law and legal state could not exist. On the other side, the rule of law has counter-influence on the application of the said principle. The same can be said for the principle of the rule of law. If the principle of constitutionality and legality is not consistently applied, there are no preconditions for the functioning of the legal state and rule of law. Moreover, legal state assumes the rule of law and the rule of law assumes the existence of legal state. In one word, these are the principles whose meaning is interconnected and whose application presumes the action on behalf of both. Otherwise, the goals and values of the legal order could not be achieved" (Kulić & Kulić, 2015, p. 168).

3. Constitutionality and legality

Constitutionality and legality are important legal principles "without which a legal state could not exist – they are the precondition, but also a tool (instrument) for achieving it. As the legal state has its legal and meta-legal meaning, thus these principles have their legal and political content. In legal sense, constitutionality and legality indicate that a legal order has certain character and quality where the constitution and laws are superior to all other lower legal acts and regulations. In such a legal order there is a hierarchy of legal acts and regulations; on the top of this hierarchy stands the constitution with laws as a supreme legal act, where the constitution itself is a law, the supreme law of the country" (Mihajlović, 2009, p. 568).

In accordance to Article 3 of the Constitution of the Republic of Serbia (2006), the rule of law is a fundamental prerequisite for the Constitution which is based on inalienable human rights. The rule of law shall be exercised through free and direct elections, constitutional guarantees of human and minority rights, separation of power, independent judiciary and observance of Constitution and law by the authorities. Also, Article 1 of the Constitution of the Republic of Serbia foresees that Republic of Serbia is a state of Serbian people and all citizens who live in it, based on the rule of law and social justice, principles of civil democracy, human and minority rights and freedoms, and commitment to European principles and values (see also: Radovanović, 2020, p. 87).

Therefore, the crucial characteristics of the principle of constitutionality are the need to harmonize laws and other internal legal acts with the Constitution and accountability of government bodies and their employees to the legal norms which constitute these legal acts. Nikolić (1997) believes that "constitutionality is just a higher form of legality, or legality raised to a higher level" (p. 351).

The new Constitution of the Republic of Serbia, according to Slavnić (2007) "was not accidently adopted in our new history, but it is rather a historical fact – it was adopted at the threshold of new era with the goal to contribute to the consolidation of Serbia as a modern European state" (p. 25). Today "we cannot imagine a single democratic order without constitution, but also without the struggle for more consistent application of adopted constitution which contains basic ideas and principles of the given society" (Kovačević, 2011, p. 217).

As we can conclude from the introductory words, the need to have clearly defined and transparent rules of conduct in a social community is "one

of key milestones in the development of humanity" (Ćupić, 2014, p. 1). The idea to establish and comply with generally accepted rules in a community became prominent in the 12th century when the first written constitutions were adopted across Europe and then in America. It is worth mentioning that the US Constitution from 1787 is considered, in theory, to be the first written constitution adopted by a modern state.

Constitutionality as a legal principle, in its normative meaning is the necessary prerequisite for establishing a legal state. It is binding for the state authority, it restricts and controls its actions, introduces obstacles for arbitrary actions, brings stability into legal order and creates basic conditions for equality and security of citizens in a legal system. Constitutionality as a legal principle, at the same time reflects an institutionalized demand for the protection of democracy and democratic order measured by human rights and freedoms enjoyed by its citizens" (Pajvančić, 2005, p. 7). Thus, "the creator of a normative theory, Hans Kelsen, understands constutionality as the principle of hierarchy of legal acts where lower legal norms are derived from superior ones, all the way up to the constitution, as the supreme legal norm" (Kovačević, 2011, p. 218).

The constitution is an "act of constituting a state on the principles of rule of law and legal state governed by the idea to have combined in one place, in one or more legal acts, all crucial rules related to the existence and functioning of one social and political organization. Although the initial role of the constitution was to regulate basic postulates, premises and principles of state's legal order, time has shown that it cannot survive without efficient system whose aim is to control and protect constitutionality and ensure complete and consistent compliance with both the essence and spirit of constitutional norms by preserving its supremacy and highest legal power" (Ćupić, 2014, p. 1). This is important to underline bearing in mind that "law in books and law in action can be two completely separate things" (Jovičić, 2006, p. 281).

As it has been emphasized by Petrović (2007), "legal and political nature of contemporary constitutions is the result of a long evolutionary development and increasing complexity of their characteristics which together have had great influence on creating and shaping the structure and character of the constitution as a legal act which, owing to being highly important for the functioning of a legal and political system, is often viewed as the indicator of the country's overall level of political culture, democratization and modern flows in its society" (p. 127). Therefore, Kovačević (2011) underlines that "the principle of constitutionality allows stability and security in a society" (p. 217).

Besides the principle of constitutionality, the principle of legality also plays an important role in all democracies.

The principle of legality has found an important place in many scientific reviews, discussions, doctrinary approaches, etc. It can be said that "legality either underlines the dynamic legal principle it pertains to, the efficiency of legal order, or the state and quality of the given law" (Mitrović, 2004, p. 57; see more on: Mitrović, 1996).

It is believed that the concept of legality in legal theory was originally established in German legal literature in 1873 by two theoreticians – Paul Laband and Karl Edwin Luthold (Garner, 1979).

Legality assumes "harmonization of bylaws and other (general and particular) legal acts with law, as well as compliance of people and legal subjects with legal norms contained in these acts. This harmonization must be achieved in both formal and material sense since law does not regulate only the form, but also the content of bylaws and other lower legal acts, both of general and particular nature. Of course, this harmonization is not always precise, particularly when we speak about the content of lower legal acts. In many cases it is done in principle. However, there are legal acts which are specific in nature and their form and content must be regulated in more details" (Kulić & Kulić, 2015, p. 169).

The most famous view on law and legality was presented by French legal scholar Leon Duguit in the first decades of the 20th century. According to him, "legal rule represents the basis of every legal system, while it is on the principle of legality to ensure its efficiency in such a way that no government body can pass a single decision which is not in compliance with previously adopted general norms, or, in another form, a single decision can be passed only within the scope which is determined by previously adopted substantive law. The essence of this principle is to provide protection of individual citizens whereas it does not make or cannot make, or must not make any exception" (Mitrović, 2014, p. 142).

Legality is "one of the key principles of legal order, which is the reason why it of crucial importance that we should take care of it and make sure that legal norms contained in the legal acts of lower legal force are harmonized with the norms from superior legal acts. If a legal act is unlawful, it means that it violates the legal order and interrupts its smooth functioning" (Kulić & Kulić, 2015, p. 170). Moreover, "long-term compliance with the principle of legality creates necessary stability of the state authority. Also, the consistent application of the principle of legality generates legal security. Legal security, in both subjective and objective sense, can exist only if the work of government

bodies and citizens' actions are regulated by previously prescribed rules which are being invariably applied" (Zekavica, 2018, p. 110).

In that context, "as a theoretical antipode of legal state, there is a police state which is most commonly defined as a state where the principle of legality has been replaced with the principle of purposefulness, a state in which the law is not applied to all people equally and where the authority and political decisions are not based on previously adopted rules, but on arbitrary will of individuals whose decisions in most cases are passed for political reasons. This state of facts leads to disappearance of elementary conditions for the establishment of a legal state with the rule of law" (Zekavica, 2018, p. 110).

Legality can be viewed in both formal and material sense. In order for a legal act to be considered lawful in a formal sense, it is necessary to be adopted by the authorized body in accordance to the rules governing its adoption and in an adequate legal form. On the other side, a legal act is lawful in a material sense if its legal norms are in compliance with the norms contained in the acts of superior legal force.

In addition to the fact that "legality assumes the relation with the particular law and that it reflects supremacy of law, it comprises (in all legal systems, including ours) some other legal elements and guarantees, such as: compliance of public and other office holders with law, publishing of laws and other legal acts before their entry into force, then, so called *vacatio legis,* the period between the announcement of the legal act and its entry into force, prohibition of retroactive application of law, the use of mother tongue in a legal proceeding, etc." (Nikolić, 1997, p. 355).

However, the principle of legality has "its political implications and meaning which is why it follows all constitutional and democratic political systems, or is one of prerequisites for democratism" (Đorđević, 1978, p. 346). In this "political and democratic sense, legality is the synonym for the rule of law which denies arbitrariness and calls for accountability of everyone whose actions are not in compliance with law" (Mihajlović, 2009, p. 571). This notion of legality, according to Đorđevića (1978), "is identified with such a legal system, or such a relationship between the authority and individuals (and such an exercise of public offices) that are based on the supremacy of law which opposes arbitrariness, as well as on the status of public authority as a public service, and the status of individuals who are allowed to do what they wish provided they do not violate laws and rights of other" (p. 347).

4. Instead of concluding remarks

As we have pointed out at the beginning of this paper, the rule of law as an idea, is one of the oldest and most significant ones in the history of legal and political thought. Contemporary understanding of the work of esteemed legal theoreticians underlines and upholds the stand that the idea of the rule of law has a significant position in the views that have been publicly expressed on the topics related to the state and law, politics and economy. The rule of law, as an ideal to strive towards, has been contemplated by all leading authors of contemporary thought – jurists, economists, politicians. However, general legitimacy of the principle of the rule of law, does not mean that it does not face multiple challenges and problems.

The discourse on the principles of constitutionality and legality has always been the cornerstone and pillar for emphasizing the importance of the rule of law in contemporary legal orders. This is particularly important if we take into account that constitutionality and legality are vital principles a state cannot exist without. They are the precondition, but also an instrument for achieving it. In that sense it should be underlined that the rule of law essentially presumes the strict compliance with the principles of constitutionality and legality, democratic elections and democratic organization of government which will consistently apply the principle of separation of power, independent judiciary, respect of human rights and freedoms and the existence of a moderate and power-restricted executive branch.

Logarušić Dejan
Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, Srbija

Rapajić Milan
Univerzitet u Kragujevcu, Pravni fakultet, Kragujevac, Srbija

ZNAČAJ I POVEZANOST NAČELA USTAVNOSTI I ZAKONITOSTI SA PRAVNIM PORETKOM I VLADAVINOM PRAVA

APSTRAKT: Vladavina prava kao ideja jedna je od najstarijih i najznačajnijih ideja u istoriji pravne i političke misli. Savremeno shvatanje uvaženih teoretičara uveliko je na stanovištu koje ističe i potvrđuje da ideja

vladavine prava zauzima ključno mesto u transparentno iznetim stavovima o državi i pravu, politici i ekonomiji. Vladavinu prava, kao ideal kome treba da se teži, vide svi vodeći autori savremene misli – i pravnici, i ekonomisti i političari. Diskurs o principima ustavnosti i zakonitosti uvek je oslonac i temelj u isticanju značaja vladavine prava u savremenom pravnom poretku. Ovo je naročito značajno ako se ima u vidu da su ustavnost i zakonitost bitni pravni principi bez kojih nema pravne države. U radu se, shodno temi, analizira nekoliko važnih pitanja – kako opredeliti značaj međusobnog saglasja i povezanosti načela ustavnosti i zakonitosti i vladavine prava, zatim, kako konceptualno predstaviti suštinu ustavnosti, potom zakonitosti, te vladavine prava i pravne države.

***Ključne reči**: vladavina prava, pravna država, ustavnost, zakonitost, teorija prava.*

References

1. Avramović, D. (2010). Vladavina prava i pravna država – istost ili različitost [The rule of law and the rule of law – sameness or difference]. *Zbornik radova Pravnog fakulteta u Novom Sadu*, *44*(3), pp. 421–437
2. Čavoški, K. (1994). *Pravo kao umeće slobode – Ogled o vladavini prava* [*Law as an art of freedom – An essay on the rule of law*]. Beograd: Službeni glasnik
3. Ćupić, D. (2014). *Ocena ustavnosti akata i radnji sudske vlasti – doktorska disertacija*. [*Evaluation of the constitutionality of acts and actions of the judicial authority – Doctoral dissertation*]. Beograd: Pravni fakultet Unverziteta u Beogradu
4. Đorđević, J. (1978). *Ustavno pravo* [*Constitutional law*]. Beograd: Savremena administracija
5. Garner, F. A. (1979). *Administrative Law*. London: Butterworth & Co Publishers Ltd.
6. Jovičić, M. (2006). *Ustav i ustavnost – o ustavu, izabrani spisi, knjiga 3* [*Constitution and Constitutionality – On the Constitution, Selected Writings, Book 3*]. Beograd: Službeni glasnik
7. Karbonije, Ž. (1992). *Pravna sociologija* [*Legal sociology*]. Novi Sad: Izdavačka knjižarnica Zorana Stojanovića
8. Kelzen, H. (1951). *Opšta teorija prava i države* [*General theory of law and the state*]. Beograd: Arhiv za pravne i društvene nauke

9. Kovačević, N. (2011). Značaj kontrole ustavnosti. *Glasnik Advokatske komore Vojvodine*, *83*(4), pp. 217–234
10. Kulić, Ž., & Kulić, M. (2015). *Uvod u pravo* [*Introduction to law*]. Brčko Distrikt: Evropski univerzitet Brčko Distrikta
11. Mandić, I. (2017). Oblici neprava determinisani spoljašnjim elementima prava [Forms of injustice determined by external elements of law]. *Glasnik Advokatske komore Vojvodine*, *88*(1), pp. 5–16
12. Mihajlović, V. (2009). *Ustavno pravo* [*Constitutional law*]. Kraljevo: V. Mihajlović
13. Mitrović, D. (1996). *Načelo zakonitosti – pojam, sadržina, oblici* [*The principle of legality – Concept, content, forms*]. Beograd: Pravni fakultet Univerziteta u Beogradu
14. Mitrović, D. (2004). Načelo zakonitosti [The principle of legality]. *Anali Pravnog fakulteta u Beogradu*, *52*(1-2), pp. 55–78
15. Mitrović, K. (2014). Učenja dva velika svetska sistema prava o zakonitosti i njihovo približavanje [The teachings of the two great world legal systems on legality and their convergence]. *NBP. Nauka, bezbednost, policija*, (2), pp. 137–151
16. Nikolić, P. (1997). *Ustavno pravo* [*Constitutional law*]. Beograd: Poslovni biro, d.o.o.
17. Pajvančić, M. (2005). *Srbija između ustava i ustavnost* [*Serbia between the constitution and constitutionalism*]. Beograd: Helsinški odbor za ljudska prava u Srbiji
18. Petrović, D. (2007). *Novi Ustav i savremena Srbija* [*The New Constitution and Modern Serbia*]. Beograd: Institut za političke studije
19. Prica, M. (2018). Jedinstvo pravnog poretka kao ustavno načelo i zakonsko uređivanje oblasti pravnog poretka – ujedno izlaganje o unutrašnjem pravnom sistem [The unity of the legal order as a constitutional principle and the legal regulation of the area of the legal order – at the same time, an exposition on the internal legal system]. *Zbornik radova Pravnog fakulteta u Nišu*, *57*(78), pp. 103–125
20. Radovanović, D. (2020). Ustavnopravni okvir prava na rad žena i muškaraca [The constitutional legal framework of the right to work for women and men]. *Pravo – teorija i praksa*, *37*(1), pp. 87–98
21. Slavnić, Lj. (2007). Ustavni sud Srbije u novom Ustavu Srbije [The Constitutional Court of Serbia in the new Constitution of Serbia]. *Pravo – teorija i praksa*, *24*(5-6), pp. 25–35
22. Šmit, K. (2003). *Tri vrste pravnonaučnog mišljenja* [*Three types of juridical opinion*]. Beograd: Dosije

23. Tadić, Lj. (1996). *Filozofija prava* [*Philosophy of law*]. Beograd: Zavod za udžbenike i nastavna sredstva
24. Ustav Republike Srbije [Constitution of the Republic of Serbia]. *Službeni glasnik RS*, br. 98/06 i 115/21
25. Zekavica, R. (2018). *Ideja vladavine prava – od antičkih korena do savremene pravne teorije i prakse* [*The idea of the rule of law – from ancient roots to contemporary legal theory and practice*]. Beograd: Kriminalističko-policijska akademija

Varađanin Tanja[*]
https://orcid.org/0000-0003-0070-3446
Stanković Marija[**]
https://orcid.org/0000-0001-7171-4439
Stanković Marko[***]
https://orcid.org/0000-0002-4238-479X

UDK: 347.3:341.222
Review article
DOI: 10.5937/ptp2502102V
Received on: April 28, 2025
Approved for publication on:
June 2, 2025
Pages: 102–112

DIFFERENCES BETWEEN CIVIL AND CRIMINAL LIABILITY

ABSTRACT: Liability denotes the capacity of a legally competent person to distinguish permitted from prohibited acts and accordingly to be held accountable for them. Beyond the term "liability" itself, there are numerous distinctions between civil liability and criminal liability. Practically, the purpose of liability is diametrically opposed. To be liable means to bear the appropriate consequences for one's conduct. Accordingly, whether referring to civil liability or criminal liability, the essence of both legal responsibilities lies in enduring the consequences arising from the actions of the liable party. The aim of this paper is to comprehensively and systematically, yet concisely and authentically, highlight the fundamental and most significant differences between these types of liability, also addressing, within civil liability, the distinctions between contractual and tortious (non-contractual) liability. Through reasoned explanations, derived conclusions, and detailed analysis of statutory provisions and judicial decisions, the key differences among these liabilities will be elucidated—an endeavor important for both theoretical scholarship and judicial practice.

[*] LLD, Assistant Professor, University Business Academy in Novi Sad, Faculty of Law for Commerce and Judiciary in Novi Sad, Novi Sad, Serbia, e-mail: tanja.varadjanin@pravni-fakultet.info
[**] LLD, Assistant Professor, University Business Academy in Novi Sad, Faculty of Law for Commerce and Judiciary in Novi Sad, Novi Sad, Serbia, e-mail: marija.stankovic@pravni-fakultet.info
[***] LLD, Associate Professor, University Business Academy in Novi Sad, Faculty of Law for Commerce and Judiciary in Novi Sad, Novi Sad, Serbia, e-mail: marko.stankovic@pravni-fakultet.info

Keywords: *civil liability, criminal liability, contractual liability, non-contractual liability.*

1. Introduction

Civil liability and criminal liability are two distinct forms of legal responsibility that may arise either concurrently or independently of one another. In earlier times, civil and criminal liability were understood as stemming from a single basis of responsibility, but this view has gradually been abandoned. According to Professor Dr. Jovan Jakšić, the wrongdoer was originally subjected to private vengeance, that is, the talion system; this was later replaced by a system of compensation, whereby, instead of physical retaliation against the offender, the injured party demanded a monetary sum depending on the circumstances of the case (Radišić, 2021, p. 207). Subsequently, the state assumed the role of determining the amount of compensation, whereby, over time, punishment and indemnification became progressively separated (Radišić, 2021, p. 207).

The distinctions between civil liability and criminal liability are both numerous and significant. Linguistically, they share the term "liability," which in its broader sense conveys a negative connotation for the person in question. To be liable means to bear the appropriate consequences. Accordingly, whether one refers to civil liability or criminal liability, the essence of both types of legal responsibility lies in enduring the consequences that constitute discomfort or hardship for the liable party.

Modern conceptions regard civil liability primarily as an obligation to compensate for damage, as derived from the statutory definition in Article 154(1) of the Law on Obligations (1978) (hereinafter "LOO"): "Whoever causes damage to another person is obliged to compensate it, unless he proves that the damage occurred without his fault." This provision merely specifies what is to be understood by "damage," without offering a conceptual definition a common approach, as most jurisdictions do not define "damage" per se within civil law. The divergence between criminal and civil liability also manifests in the nature of the norms they protect, since these norms are constructed through different regulatory methods (Salma, 2007, p. 455).

The objective of this paper is to comprehensively and systematically yet concisely and authentically highlight the fundamental and most significant differences between these two forms of liability, while also tracing, within the scope of civil liability, the distinctions between contractual and tortious (non-contractual) liability.

2. The Legal Nature of Civil and Criminal Liability

The prohibition on causing damage is a cornerstone principle of civil law. It is explicitly enshrined in Article 154 of LOO, which provides that "whoever causes damage to another person is obliged to compensate it." The statutory framework of civil law does not offer a conceptual definition of "damage," but only specifies what it encompasses. Damage is neither exhaustively enumerated nor are specific prohibited acts listed; rather, it is defined in broad terms. Nevertheless, the civil-law incrimination is not imprecise: its scope, although stated generally, is regarded as determined within sufficiently exact boundaries in the context of the prohibition on causing damage (Salma, 2007, p. 458). This primarily refers to damage as (a) diminution of another's property (actual loss) and prevention of its increase (loss of profit), and (b) the infliction of physical or psychological pain or fear on another person (non-material damage) (Article 155 LOO).

There are two categories of civil liability: contractual liability and non-contractual (tortious) liability. Although our law distinguishes non-contractual from contractual liability for damage, it brings them closer by providing that most of the provisions governing compensation for non-contractual damage apply mutatis mutandis to compensation for contractual damage (Knežević, 2010, p. 54). Contractual liability arises from breach of a contractual obligation, whereas non-contractual liability stems from the general principle prohibiting one party from causing damage to another. In contractual liability, a legal relationship existed between the parties prior to the damage, while in non-contractual liability no pre-existing legal relationship is required between the tortfeasor and the injured party (Radovanov, 2008, p. 230).

By contrast, criminal liability is founded on the fundamental maxim *nullum crimen, nulla poena sine lege*, meaning that criminal offences and their penalties are exhaustively prescribed by law, thus limiting the scope of criminal liability (Radišić, 2021, p. 207).

Accordingly, civil and criminal liability are treated as two distinct forms of legal responsibility. They may arise in parallel from the same event resulting in the cumulation of delicts and of liability (Radišić, 2021, p. 207). A common example in theory and practice is theft, which gives rise to both criminal and civil liability: the offender is prosecuted criminally, and because the act diminishes someone's property, the same act also grounds a civil claim for compensation. Likewise, certain events may not constitute criminal offences yet still cause damage, thereby generating civil-law liability (Radišić, 2021, p. 207).

In legal doctrine, the principal differences in civil liability are identified with respect to (a) the incrimination or unlawfulness of the tortfeasor's act, (b) the degree of liability, (c) the prerequisites for liability, and (d) the consequences following the commission of a criminal offence or civil tort.

Within the sphere of contractual versus non-contractual liability, differences manifest in the basis of liability, the identity of the liable subject, statutory regulation, underlying principles, the extent and scope of compensable damage, and the applicable statutes of limitations for claims.

3. Liable Parties

Having previously addressed incrimination, this section offers only a brief overview and highlights the fundamental distinction between civil liability and criminal liability in the context of the principle of enumeration. Accordingly, criminal liability is narrower in scope, since criminal offences are exhaustively defined by statute. Under Article 14(1) of the Criminal Code (2005) (hereinafter "CC"), a criminal offence is an act that (a) is prescribed by law as a crime, (b) is unlawful, and (c) is committed with culpability. There can be no criminal offence if unlawfulness or culpability is excluded, even if all statutory elements are otherwise met (Article 1(2) CC).

By contrast, civil liability is broader: the range of civil delicts is far greater and is not confined to an exhaustive list (Radovanov, 2008, p. 232). Civil liability arises not only from breaches of legal provisions but also from violations of moral norms or customary practice.

In contrast to civil liability, criminal liability is governed by the rule that, "if there is no unlawful act punishable by law, then there can be no criminal liability" (Radovanov, 2008, p. 232). Civil liability, however, does not necessarily require the unlawfulness of the act. Thus, pursuant to Article 154(2) of the LOO, one is liable for damage caused by things or activities that pose an increased risk to the environment regardless of fault (objective liability).

Within civil liability, contractual and non-contractual (tortious) liability differ in that non-contractual liability is governed by imperative norms, whereas contractual liability is regulated by dispositive norms (Radovanov, 2008, p. 230). As Antić observes, "the key distinction between contractual and non-contractual liability for damage lies in the character of the norms that govern the field of liability" (Antić, 2014, p. 457). Non-contractual liability arises from the failure to observe a legal obligation that is, conduct contrary to a legal norm causing damage to another (Loza, 1981, p. 164). Contractual

liability, by contrast, results from breach of a pre-existing contractual obligation, causing harmful consequences to the other contracting party (Loza, 1981, p. 164). In statutorily permitted cases, contracting parties may, by virtue of dispositive norms, either tighten or entirely exclude civil liability for example, Article 486(1) of the LOO allows the parties to limit or exclude the seller's liability for material defects in the sold item.

One of the most salient differences between civil liability and criminal liability lies in the identity of the liable party. In criminal law, liability is strictly personal and individual (Radišić, 2021, p. 208): no one other than the perpetrator of a criminal offence may be held criminally responsible. Only the person who committed the offence can incur liability (Đurović & Dragašević, 1980, p. 140). In order to hold someone liable for a criminal offence and impose a criminal sanction (penalty), it is necessary to establish the elements of criminal liability, namely, capacity and fault. "Thus, on the basis of fault a unique relationship is formed between the criminal offence, its perpetrator, and the criminal sanction; and, when capacity is also demonstrated, a complete criminal-law relationship is achieved" (Čejović & Kulić, 2014, p. 236).

In civil liability, the responsible parties vary according to whether the claim is contractual or tortious. Under contractual liability, only legally competent persons can be held liable, since one prerequisite for a valid legal transaction is the parties' legal capacity. In tortious liability, however, even persons lacking legal capacity may be held liable for damage.

In the realm of non-contractual liability, i.e., tortious liability (terms used synonymously), the LOO prescribes cases of vicarious liability for the acts of another, as well as special instances of liability. As a general rule, the tortfeasor is liable for damage arising from his own actions. Nevertheless, the LOO provides for situations in which one person may be held liable for the acts of another (Section 3 LOO).

According to Oliver Antić, whose view is grounded in the provisions of the LOO, the classification of vicarious liability encompasses liability for the mentally ill and those of impaired mental development; parental and guardianship liability; liability for agents; liability of legal persons toward third parties; and employer liability. What is common to all forms of vicarious liability is that they constitute objective liability in a broader sense (Antić, 2014, p. 486). Accordingly, there arises a separation between the tortfeasor and the party liable for another, such that three distinct roles emerge: the injured party, the tortfeasor, and the vicariously liable person (Antić, 2014, p. 486). Non-contractual liability is broader than contractual liability because, in contractual liability for breach of a contractual obligation, namely for

non-performance or delay in performance, the other contracting party alone is liable, whereas under non-contractual liability the circle of potentially liable persons is wider.

In conclusion, the liable subjects under civil and criminal liability are strictly prescribed by law, with clear, exact, and fundamental differences between them.

4. Degree of Liability – Fault

Fault (lat. culpa) is understood broadly as "guilt." Civil law distinguishes between liability based on fault (subjective liability) and liability irrespective of fault (objective liability). The subjective theory seeks to explain why the tortfeasor caused harm, focusing on the tortfeasor's internal attitude toward the injurious act. In contrast, the objective theory compares the tortfeasor's conduct to the legal norm and assesses whether that conduct deviates from what is expected.

In both legislation and legal doctrine, fault is further classified as presumed fault versus proven fault (Radovanov, 2008, p. 262). This distinction underpins another difference between contractual and non-contractual liability: contractual liability operates on the basis of presumed fault, whereas non-contractual (tortious) liability incorporates both presumed and proven fault.

Under criminal law, fault requires the perpetrator's psychological concurrence with the criminal act and a specific mental attitude toward its consequences (Čejović & Kulić, 2014, p. 172). In criminal proceedings, fault must be proven, and the accused enjoys a presumption of innocence until proven otherwise.

A key distinction between civil and criminal liability lies in the degree of fault. Legal doctrine divides fault into intent (*dolus*) and negligence (*culpa*). "*Dolus is further subdivided into dolus directus and dolus eventualis"* (Antić, 2008, p. 456). Direct intent exists when the tortfeasor desires the harmful consequence and is fully aware of it. Conditional intent (dolus eventualis) arises when the tortfeasor foresees the possible harmful outcome, does not wish it, but nevertheless accepts it and persists in the dangerous conduct (Antić, 2008, p. 456).

By contrast, negligence may be gross or ordinary. Gross negligence occurs when the tortfeasor fails to act as a reasonably careful person would and behaves in an extremely careless manner (Đorđević & Stanković, 1974, p. 325). Ordinary negligence exists when the tortfeasor fails to act

as a reasonably careful person but without reaching the threshold of gross negligence (Đorđević & Stanković, 1974, p. 325).

In civil liability, the tortfeasor may be held liable for negligence per se, whereas in criminal liability negligence gives rise to liability only if expressly provided by law. In criminal law, the mental element manifests either as intent or as negligence (Čejović & Kulić, 2014, p. 172). Under Article 25 CC, an offence is committed with intent when the perpetrator is aware of and wills the act, or foresees its possibility and reconciles with it. Under Article 26 CC, an offence is committed by negligence when the perpetrator either foresees the possibility of committing the offence but recklessly assumes it will not occur or when the perpetrator fails to foresee the possibility, despite it being objectively foreseeable under the circumstances.

Accordingly, intent in civil liability and intent in criminal liability are similarly defined, while a major difference lies in the treatment of negligence: Article 22(2) CC provides that criminal liability for negligent offences exists only where the law so provides.

Finally, another distinction from criminal liability is the existence of an institute of divided liability in civil law. Conversely, under Article 33 CC, criminal law prescribes that where two or more persons jointly commit an offence whether by acting with intent together or by one person's intentional act materially contributing to the offence they are each punishable as principals. Thus, under the Code, an accused cannot be partially guilty: one either is guilty of the offence or is not, even when multiple persons participate in its commission.

5. Sanctions

One of the fundamental differences between civil liability and criminal liability lies in the consequences that follow the occurrence of a harmful event whether a civil tort or a criminal offence. Criminal law places emphasis on the degree of fault, whereas civil law determines the amount and scope of damages regardless of fault.

"In criminal law, the measures applied against perpetrators of criminal offences are called criminal sanctions." Under Article 4(1) of the CC, criminal sanctions are exhaustively listed as penalties, warning measures, security measures, and educational measures. The Code also prescribes the purpose of criminal sanctions, namely the protection of individuals and other fundamental social values to the extent necessary to suppress offences. The aim of a particular sanction depends on its type, and the court assesses each

case individually. Individualization of criminal sanctions means tailoring the sanction to the particular characteristics of the offender and the offence, with a view to fully achieving the purposes of criminal sanctions (Čejović & Kulić, 2014, p. 287). Thus, factors such as the length of imprisonment or the amount of a fine hinge significantly on the offender's mental attitude toward the offence whether they were aware of and willed the act and its consequences (Salma, 2007, p. 458).

By contrast, LOO is founded on the principle of full compensation for damage (Salma, 2007, p. 458). The quantum of damages equals the amount of compensation. Historically, the measure of compensation depended on the form of fault: if the tortfeasor caused damage intentionally, they were liable for both actual loss and loss of profit; if the damage was caused by negligence, liability was limited to actual loss and did not extend to loss of profit.

Modern doctrine has abandoned this fault-based assessment and holds that the quantum of damages is determined independently of the degree of fault. Article 155 LOO specifies what constitutes "damage," entitling the injured party to compensation for both material and non-material harm. The injured party may claim actual loss and loss of profit. Compensation for material damage is principally awarded in natura, or, if that is not possible, in monetary form. If the injured party suffers complete or partial incapacity for work, loses earnings accordingly, incurs permanently increased needs, or has their prospects for further development and advancement destroyed or diminished, the liable party must pay an annuity as compensation (Article 195(2) LOO). By contrast, non-material damage is ordinarily quantified in monetary terms. However, Article 199 LOO provides that, in cases of infringement of personality rights, the court may order, at the tortfeasor's expense, publication of the judgment or correction, withdrawal of the offending statement, or other measures necessary to achieve the purpose of compensation.

In the context of contractual liability, the creditor is entitled to actual loss and loss of profit, provided that the debtor, at the time of contracting, ought to have foreseen those losses as possible consequences of breach (Radovanov, 2008, p. 231).

6. Concluding Remarks

It is concluded that the differences between civil liability and criminal liability are highly demanding, inexhaustible, and complex; they can always be analyzed in greater detail. Both forms of liability may arise in parallel or independently of one another.

Today, we witness an increasing frequency of parallel legal liabilities due to technical-technological developments and innovation projects. Likewise, traffic accidents the most common grounds for both civil and criminal liability occur ever more often. A single course of conduct may give rise to criminal liability while simultaneously constituting the basis for a civil claim for damages.

Pursuant to Article 13 of the Law on Civil Procedure (2011), a court deciding on civil claims is bound, with respect to the existence of a criminal offence and the offender's criminal liability, by the final judgment of the criminal court in which the accused is convicted.

A noteworthy and frequent example in case-law is driving with an intoxicated driver. As held by the Appellate Court in Belgrade, case no. Gž. 5085/2012 of 6 December 2012:

"The injured party who consented to be driven, knowing that the driver was intoxicated, contributed to the occurrence of harmful consequences in the traffic accident caused by the intoxicated driver."

The reasoning continues:

"According to the facts established at first instance and the records in the criminal file, the traffic accident was preceded by socializing between the prosecutor and S. S., during which both consumed alcohol immediately before the incident. Given that the prosecutor who testified as the injured party undoubtedly knew that S. S. had consumed alcohol and did not possess a driving licence, by agreeing to ride with him in that condition he consciously assumed the risk of possible harmful consequences. Accordingly, the degree of the prosecutor's contribution to the resulting harm is assessed at 40 percent."

Thus, the civil court and the criminal court weigh the relevant circumstances differently in order to reach the most just and correct decision. These circumstances vary according to each individual case.

Accordingly, if the criminal court convicts multiple persons equally for the same offence that also caused damage, the civil court is not bound by that decision when determining the amount and scope of damages. It is entirely possible for a person to be acquitted of criminal liability yet still held civilly liable for the property damage suffered. In relation to a civil claim for damages arising from a criminal offence, the criminal court may either rule on the claim itself or refer the injured party to file a separate civil action.

Varađanin Tanja
Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, Srbija

Stanković Marija
Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, Srbija

Stanković Marko
Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, Srbija

RAZLIKE IZMEĐU GRAĐANSKOPRAVNE I KRIVIČNOPRAVNE ODGOVORNOSTI

APSTRAKT: Odgovornost predstavlja sposobnost poslovno sposobnog lica da razlikuje dozvoljene od nedozvoljenih radnji i da shodno tome, za njih i odgovara. Osim reči „odgovornost" razlike između građanskopravne i krivičnopravne odgovornosti su mnogobrojne. U praktičnom smislu, smisao odgovornosti je dijametralno suprotan. Biti odgovoran znači snositi odgovarajuće posledice za svoje delacije. Shodno tome, bilo da je reč o građanskopravnoj odgovornosti ili pak o krivičnoj odgovornosti, suština obe pravne odgovornosti jeste u trpljenju posledica koje su nastale delacijom odgovornog lica. Cilj rada je da se na sveobuhvatan i sistematski način, koncizno i autentično ukaže na osnovne i najvažnije razlike predmetnih odgovornosti provlačeći, u okviru građanskopravne odgovornosti, i pojedine razlike između ugovorne i deliktne (vanugovorne) odgovornosti. Argumentovanim objašnjenjima i izvedenim zaključcima, kao i detaljnom analizom zakonskih rešenja i rešenja iz sudske prakse, ukazaće se na ključne razlike predmetnih odgovornosti, a što je od važnosti kako za teorijsku, tako i za sudsku praksu.

Ključne reči: *građanskopravna odgovornost, krivičnopravna odgovornost, ugovorna odgovornost, vanugovorna odgovornost.*

References

1. Antić, O. (2014). *Obligaciono pravo* [*Law of Obligations*]. Beograd: Pravni fakultet
2. Antić, O. (2008). *Obligaciono pravo* [*Law of Obligations*]. Beograd: Pravni fakultet
3. Knežević, M. (2010). Opšta pravila odgovornosti [*General rules of responsibility*]. *Pravo – teorija i praksa*, *27*(5–6), pp. 42–61
4. Loza, B. (1981). *Obligaciono prvo – opšti deo* [*Law of Obligations – general part*]. Zenica: Dom Štampe
5. Radišić, J. (2021). *Obligaciono pravo – opšti deo* [*Law of Obligations – general part*]. Niš: Pravni fakultet Univerziteta u Nišu
6. Radovanov, A. (2008). *Obligaciono pravo – opšti deo* [*Law of obligations – general part*]. Novi Sad: Pravni fakultet za privredu i pravosuđe Univerzieta Privredna akademija u Novom Sadu
7. Salma, J. (2007). *Obligaciono pravo* [*Law of Obligations*]. Novi Sad: Pravni fakultet Univerziteta u Novom Sadu
8. Čejović, B., & Kulić, M. (2014). *Krivično pravo* [*Criminal law*]. Novi Sad: Pravni fakultet za privredu i pravosuđe Univerziteta Privredna akademija u Novom Sadu
9. Đurović, R., & Dragašević, M. (1980). *Obligaciono pravo sa poslovima prometa.* [*Obligations law with traffic matters*]. Beograd: Savremena administracija
10. Đorđević, Ž., & Stanković, S. (1974). *Obligaciono pravo – opšti deo* [*Law of obligations – general part*]. Beograd: Savremena administracija
11. Zakon o obligacionim odnosima [Law on Obligations]. *Službeni list SFRJ,* br. 29/78, 39/85, 45/89 – odluka USJ i 57/89, *Službeni list SRJ*, br. 31/93, *Službeni list SCG,* br. 1/03 – *Ustavna povelja i Službeni glasnik RS,* br. 18/20
12. Krivični zakonik [*Criminal Code*]. *Službeni glasnik RS*, br. 85/05, 88/05 – ispr., 107/05 – ispr., 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19 i 94/24
13. Zakon o parničnom postupku [Law on Civil Procedure]. *Službeni glasnik RS,* br. 72/11, 49/13 – odluka US, 74/13 – odluka US, 55/14, 87/18, 18/20 i 10/23 – dr. zakon

Spasojević Đorđe[*]
https://orcid.org/0000-0002-4645-8477
Prelević Plavšić Snežana[**]
https://orcid.org/0009-0002-8869-9292
Vlajnić Jelena[***]
https://orcid.org/0000-0003-4869-7102

UDK: 342.7:323.28
Review article
DOI: 10.5937/ptp2502113S
Received on: February 26, 2025
Approved for publication on:
May 16, 2025
Pages: 113–129

THE SUBCULTURE OF CLOTHING BETWEEN HUMAN RIGHTS AND THE THREAT OF TERRORISM

ABSTRACT: Although at first glance clothing choices appear to be a matter of individual freedom—subject only to certain exceptions involving unwritten, or more rarely written, norms that typically carry no serious sanctions—there are situations in which this issue is raised to a much higher level. It is often linked to specific garments associated with Muslim women, such as the hijab, niqab, burqa, and others. In line with this, the paper highlights certain challenges related to human rights issues, but also to security concerns, which require a more in-depth and nuanced approach, especially considering numerous instances in which men dressed as women have carried out terrorist attacks or evaded law enforcement. In order to propose a suitable legal solution—a compromise that would respect individual rights while also addressing potential security risks—the paper employs several methodological approaches. A comparative method is used to examine the legal frameworks of different countries. Documentary analysis is applied to judgments of the European Court of Human Rights. Additionally, an analytical approach is used to examine relevant passages

[*]LLD, Assistant Professor, Faculty of Business Economics and Entrepreneurship, Belgrade, Serbia, e-mail: spasojevic.djordje@gmail.com
[**]LLD, Assistant Professor, Faculty of Business Economics and Entrepreneurship, Belgrade, Serbia, e-mail: jel.vlajnic@gmail.com
[***]LLD, Assistant Professor, Faculty of Business Economics and Entrepreneurship, Belgrade, Serbia, e-mail: snezaprelevic@yahoo.com

from the Qur'an that pertain to clothing and the obligation to cover certain parts of the body.

Keywords: *human rights, terrorism, female terrorists, security, European Court of Human Rights.*

1. Introduction

As is the case with many spheres of life, we can say that terrorism is characterized by many prejudices. This especially applies to female terrorists, considering that when terrorism is mentioned in the general public, among the first associations is a man with a distinctive appearance, of the Islamic faith. On the contrary, in the context of terrorism, women were often associated with some other terms, such as, for example, human trafficking as a form of financing terrorism, given the numerous cases in which, for this reason, "they were taken by fraud or force and sold to work in forced prostitution" (Bjelajac, Matijašević & Dimitrijević, 2012, p. 395).

Although in recent years, in the majority of cases, men undertake terrorist attacks, women and children are increasingly mentioned in the context of carrying them out, even though they were traditionally spoken of primarily as victims (Dabić, Spasojević & Radulović, 2023; Prelević Plavšić, Spasojević & Dragojlović, 2023). One must not ignore the fact that Islam, according to certain, extreme interpretations, foresees a "reward" for men, but also for women who undertake a suicidal terrorist attack. Accordingly, men will be welcomed in paradise by seventy-two virgins[1], and women will be massaged with scented oils by young men wrapped in towels (Petrović, 2018, p. 70).

The statement that women's terrorism is a recent phenomenon should be approached with great caution and extremely conditionally. Apart from the numerous examples of attacks undertaken by them, some of which are more than a century old, the component that additionally relativizes the given allegations refers to the question of how broadly "women's terrorism" should be interpreted as a phrase. If we were to approach the mentioned issue to an extremely extensive extent, under this phrase we could subsume the role that women play as mothers in the indoctrination of children, through raising and

[1] In certain situations, the mentioned award is viewed quite sarcastically, as was the case in 2005 in Denmark in the newspaper "Jyllands-Posten". On that occasion, in the given newspaper, a caricature of the prophet Muhammad was shown, standing on a cloud, telling the suicide bombers who are waiting in line to enter heaven to return, because there are no more virgins in it, so they cannot be admitted (Vuković, 2018, pp. 139–140).

educating them (de Leede, 2018, p. 1). In accordance with this approach, it should be noted that terrorists often see female members of their organizations as targets for rape, and even mere "cannon fodder" (Spasić & Vučković, 2011, p. 263). In contrast, the extremely restrictive approach, which is particularly characteristic of the general public, almost equates female terrorism with suicide bombings.

It would not be correct to equate female terrorism with suicide bombings, especially if we did so because of the specific, conservative dress code of women of the Islamic faith. On the contrary, there are examples of attacks of this type, for which it cannot be said that there is a correlation between the wearing of said clothes and their execution.[2] Nevertheless, taking into account the frequency of such attacks, which can be directly linked to the misuse of the aforementioned clothing, primarily by female terrorists, but also by male perpetrators, this problem should be approached with a lot of attention.

Accordingly, it needs to be approached from several angles. Apart from the religious aspect, i.e. the review and analysis of the relevant chapters of the Qur'an, certain comparative legal solutions regarding the prohibition of wearing some of the aforementioned items of clothing, as well as the practice of the European Court of Human Rights, deserve special attention. In the search for an adequate, balancing normative approach, we will analyze the comparative legal solutions of individual countries, guided by several criteria when selecting them. On the one hand, we would like to point out the variety of reasons that were guided by the legislators of individual countries, among which those related to the security aspect, as well as those related to women's equality, stand out. On the other hand, we believe that, bearing in mind the transnational nature of terrorism, we should take into account the normative solutions of individual European countries as well as those from other continents. In other words, the transnational character of terrorism should be viewed not only through the prism of terrorists and their attacks, but also through the prism of the necessity of fighting against them in the normative field, which also knows no borders. At the same time, one should not be prejudiced when it comes to countries whose legal systems are not among the developed ones, since this fact does not necessarily mean that such systems cannot have certain solutions that deserve attention and that can represent a good basis for the action of our legislator. The selection of cases from the practice of the European Court of Human Rights, which we will analyze, was

[2] In a case dating back to 1985, sixteen-year-old Sana Kudali killed two Israeli soldiers while driving a truck loaded with explosives (Zedalis, 2005).

made considering that they represent an adequate example of the application of the principle of proportionality between respect for religious freedom and respect for the interests of public security, which is dominantly derived from the decisions of the aforementioned court, which also represents a type of balancing approach. Analyzing one of the cases, we will draw attention to the existence of similar problems among members of other religions, which concern the respect of the right to freedom of religion, in the context of the justification of short-term removal of certain items of clothing, for the sake of public safety, as well as to the fact that in this case, continuity can be observed in the observance of the aforementioned principle of proportionality.

2. "Clothing as a terrorist threat", some comparative legal solutions and a proposal *de lege ferenda* for domestic legislation

As was the case much earlier with Christian states, not even individual Islamic states remained immune to the influence of secularism. However, a large number of cases from practice testify that the aforementioned influence did not lead to a decrease in religiously based terrorism. When it comes to women, among them in recent decades, especially among those of a younger age, an increasing number of those who declare themselves as believers can be observed. Of course, such determination does not necessarily indicate belonging to terrorist organizations in the vast majority of cases. The stated religious determination can be seen in the range from returning to the traditional way of dressing, under which, among others, we can classify the hijab, which since the end of the last century has been seen more and more frequently in certain urban settlements in our country, and up to the cultivation of sympathies or even membership in terrorist organizations.

Problems often arise when distinguishing the hijab from clothing items such as the burqa and the niqab. Hijab is a scarf that covers the hair, head and neck, while the face is completely uncovered. The niqab is a fabric that, apart from the mentioned parts, also covers the face, with a slit at eye level. Burka is a one-piece, the most closed way of dressing, which covers the whole body and face, with a narrow mesh in the area of the eyes.

These items of clothing can represent a convenient way of hiding cold and firearms and explosives, which, among other things, was one of the reasons for banning some of them in certain countries. For example, in 2011, France banned the wearing of the niqab and burka in public places (Družetić, 2013). At that moment, the current French president, Nicolas Sarkozy, found the justification for that step in the need to protect women and ensure equality

(Avolio & del Carpio, 2020). In addition, he cited as a reason the obligation to accept French cultural patterns, saying that those who do not do so are not welcome in France (Milošević, 2012). China, Denmark, Germany, Belgium, Italy and Spain were guided by similar or the same reasons. On the other hand, the Netherlands, Congo, Chad and Cameroon have openly and unequivocally pointed out that the reason for this is the protection of security and national interests (Simić, 2019). In early 2022, the French senate decided on a more radical, prohibitive approach, banning the wearing of the hijab during sporting events, under the rather unconvincing pretext that wearing the garment poses a risk to the safety of female competitors during performances, as reported in *Aljazeera* (2022). Reasons related to religious neutrality, i.e. secularism, are often cited as a justification for the application of a prohibitive approach (Kurtović, 2018). However, in some cases, the prohibitive approach can have a counterproductive effect, manifested in causing revolts among members of a given religion, which can ultimately lead to their radicalization and extremism. In addition to problems related to security, the prohibitive approach triggers some others such as limiting freedoms and privacy (Domazet, Marković & Skakavac, 2024), discrimination (Rašević & Vlajnić, 2022), etc.

The key question that arises is how to find a balancing solution between the right of women of the Islamic faith to be dressed in accordance with the teachings of the religion to which they belong and the need for preventive action in terms of suppressing a possible terrorist threat. When it comes to the burka and chador, their convenience for hiding cold and firearms and explosives is often pointed out in support of their ban, and that thanks to them, identification problems can arise. Regarding the first argument, we believe that it can only be partially accepted. Although this danger exists, it is not manifested to a lesser extent when wearing certain items of clothing that are not specific to members of the Islamic tradition, culture and religion, such as coats, wide and long jackets, etc.[3] If, for the purpose of risk assessment, we were to exclusively use as a criterion the suitability of hiding explosives, in that case every person who, for example, wears a coat, would represent a possible terrorist. The solution reached by Sri Lanka is a good attempt to find the aforementioned balance, bearing in mind that it prohibits covering the face, i.e. the use of the burqa and niqab, while allowing the use of the hijab

[3] Although cases of wearing suicide belts or vests under clothing that highlights the attacker's body to a greater extent, such as shirts, t-shirts, have been recorded in practice, they are still not the most suitable method of hiding explosives. In one of the cases that happened in Mosul, Iraqi soldiers noticed in time that a six-year-old boy, sent by jihadists in a suicide bombing attack, was hiding something suspicious under his shirt.

and chador. However, it is acceptable in the part concerning the hijab, but not completely in regard to the chador. A chador is a type of wide black cloak, which looks like a tent due to its dimensions. It covers the entire body, except for the face. The problem arises because it is designed in such a way that its parts can be held by hand in the area of the face (Jovanović, 2014), which in certain situations can make face identification difficult.

Unlike the mentioned countries, in the Republic of Serbia, there are no laws prohibiting the wearing of the above items of clothing, which certainly ranks our legislator among the more liberal ones. However, this does not mean that there are no security protocols in accordance with which short-term removal is allowed[4], which ultimately does not contradict our Constitution, as the highest legal act, nor with international regulations and the views of the European Court of Human Rights. We believe that our legislator should accept a modified version of Sri Lanka's decision, which would mean that wearing hijab, sheila, hijab amira, khimar and similar parts of clothing that do not cover the face, as well as chadors, should be allowed in public spaces, with the prohibition to cover the mentioned part of the body with its ends. Such a solution would represent a significant step forward in terms of security, while it would not be a disruptive factor in the field of exercising religious rights and freedoms.

3. The Qur'an and the subculture of clothing

The opinion that the wearing of hijab, shayla, hijab amirah, khimar[5] and similar parts of clothing, as well as chadors should be allowed in public spaces, with the prohibition to cover the face with its ends, which satisfies both security reasons and religious teachings, does not contradict the verses of the Qur'an.

[4] For example, some airports in Serbia, such as Niš and Kraljevo, have security protocols in accordance with which it is necessary to remove certain items of clothing during scanner control, given that, unlike the newer generation scanners that some larger airports have, they cannot scan through clothing. These are religiously neutral items of clothing, such as jackets and coats, but also those that cover the head and face. For Muslim women who do not want to remove the headscarf on the spot, a special examination room is provided, so that the violation of their privacy is reduced to the smallest, necessary measure in order to protect their dignity and integrity (Euronews Srbija, 2023).

[5] Sheila presents a long rectangular scarf, which is freely wrapped around the head and thrown over the back. Hijab amir is a two-part garment, where the first part, like a cap, covers the head, covering the same area as a classic hijab, while the second part, in the form of a sleeve, covers the back. In the case of a khimar, it is a cloak with a slit in the face, which covers the ears, hair, back and extends to the waist (Steinver, 2016).

It does not directly state which of the mentioned items of clothing are considered adequate, just as face covering is not set as an imperative. In Sura 24, it is stated: "Tell the believers to lower their gaze and take care of their private parts; that is better for them, for verily Allah knows what they do" (verse 30). "And tell the believers to lower their gaze and take care of their private parts; and let them not allow anything to be seen of their ornaments except what is external anyway, and let them lower their veils over their breasts; let them not show their ornaments to others, they can only do so to their husbands, or their fathers, or their husbands' fathers, or their sons, or their husbands' sons, or their brothers or their brothers' sons, or their sisters' sons, or their female friends, or their female slaves, or men who do not need women, or children who do not yet know what the private parts of women are..." (verse 31) (Korkut, n.d., pp. 162–163). In addition, Surah 33 reads: "O Believer, tell your wives, and your daughters, and the believing women to lower their garments and line up." That way, it will be easier to recognize them, so they won't be harassed. And Allah is Forgiving and Merciful" (verse 59) (Korkut, n.d., p. 200).

In the quoted verses, there is no mention of the necessity of covering the face, but only the breasts are directly mentioned as a part of the body, i.e. the necessity of covering them. In addition, it is emphasized that the wearing of dresses is mandatory, but there is no mention of the necessity of covering the face either.

When it comes to children and the question of when they should start wearing the hijab, the Koran does not offer a concrete answer. Experts in this field state several alternative prescribed conditions: ejaculation while awake or in a dream, growth of pubic hair, entering the fifteenth year, getting the first menstruation (Kuduzović, n.d.). Therefore, by fulfilling any of the mentioned conditions, which in the religious context are considered signs of adulthood, it is considered that the obligation to wear the hijab arises.

However, in practice, examples of wearing the hijab, but also somewhat less frequently the burka and niqab, can be found by children of a younger age. It seems that such a phenomenon should not be viewed negatively from a normative aspect, if it is about wearing the hijab, bearing in mind, among other things, the views and interpretations of certain influential Islamic theologians. For example, Kuduzović points out the need for "getting the child used to wearing loose clothes and covering the head with a headscarf", saying that "a female child should not be forced to wear the hijab, but the Islamic costume should be gradually, in a nice and acceptable way, made to come to her liking, so that when she becomes of age she accepts the obligation to wear the hijab" (Kuduzović, n.d.).

On the other hand, we believe that, as is the case with adult Muslim women, the wearing of burqas, niqabs and similar clothing items that cover the face of children who are not even considered to be of legal age in a religious context should not be viewed favorably by the legislator. Apart from the fact that such behavior has no basis in Islam itself, and for this reason, we cannot speak of a violation of religious rights, there are reasons that can be linked to problems in determining the identity of perpetrators and victims of criminal acts.

If the wearing of the burqa and niqab were allowed, it would open the door to certain types of abuse by non-Muslims as well. Taking into account the innovativeness of juvenile perpetrators, it seems that a potential problem could arise if they adapted their modus operandi in such a way that they would use the mentioned items of clothing for camouflage and thus make it difficult for the competent authorities to detect them. This could create potential problems in the field of establishing the identity of the perpetrators of theft, robbery, burglary, etc. primarily in countries where a large number of Muslims live, where the wearing of the aforementioned clothing by the younger population would be a daily occurrence. In addition, problems in the field of establishing identity could also arise when combating child trafficking, which, like human trafficking in general, is one of the most prevalent forms of financing terrorism (Bjelajac, Tepavac & Dašić, 2012, p. 240). When moving, transporting, handing over the victims, the burqa or niqab could represent a suitable means of hiding their identity, as well as possible traces of physical violence, to which they are often exposed. Bearing in mind that it is characteristic of minors and child victims of human trafficking, among other things, that they often move in public places in a group, in the presence of adults, and that they often change locations on a daily basis, crossing long distances (Alempijević, et al., 2010, p. 65), wearing the aforementioned clothing items would be a complicating factor when finding and rescuing them.

4. Practice of the European Court of Human Rights

Proponents and opponents of a complete ban on burqas and niqabs rely on different arguments based on human rights. In other words, what both of them have in common is the fact that they prioritize the protection of women's rights, but from different aspects. On the one hand, such a ban is justified by the need to protect the dignity and equal rights of women (Okin, 1997), as well as by the fact that it contributes to the preservation of public security (Chesler, 2010) and reflects national values, such as official secularism,

but also the so-called "Christian-type secularism" (Malešević, 2007, p. 19), which, although formally based on the separation of church and state, fundamentally tolerates and even sometimes promotes Christian motives in various socio-political fields. On the other hand, such a ban is criticized because it undermines women's right to equal treatment (Howard, 2012), freedom of religion (Ashni & Gerber, 2014), as well as freedom of movement and access public services (Human Rights Watch, 2009).

The existence of arguments in support of the fact that the wearing of the mentioned items of clothing should be allowed, does not mean that there are no circumstances, due to which it is justified to take them off for a short time, such as checking the identity by the competent authorities, taking photos for the preparation of personal documents, etc.

The European Court of Human Rights is of the same opinion. In the case of *El Morsli v France*, a Moroccan citizen, Fatima El Morsli, married to a French citizen, went to the Consulate General of France in Marrakesh on March 12, 2002 to apply for a visa. She was not allowed to enter the consulate because she did not agree to remove her veil for identity verification. On June 25, 2003, the Board of Appeals rejected the appeal filed on her behalf by her husband, with the explanation that the formal requirements were not met, considering that she did not comply with the regulations governing the visa issuance procedure. In a new appeal that he submitted on her behalf to the Council of State of France, which was rejected, the husband invoked the right to respect for family life, that is, the right to freedom of religion.[6] The conclusion of the European Court of Human Rights was that there was no disproportionate violation of the mentioned rights, because the measures taken were necessary in the interest of public safety and that the removal of the veil for the purpose of the security check takes a very short time.

The aforementioned opinion of the European Court of Human Rights does not apply exclusively to cases concerning members of the Islamic faith. In the case of *Phull v France*, British citizen Suku Paul, referring to Art. 9 of the European Convention on Human Rights and Art. 2 st. 4 of Protocol no. 4 of this convention, pointed to the violation of the right to freedom of religion and the violation of the right to freedom of movement. Since the person in question is a member of Sikhism, he is obliged to wear a turban on his head in accordance with the principles of this religion. When he was returning from a business trip on October 10, 2003, airport security officers insisted

[6] Fatima El Morsli v France, application no. 15585/06, judgment ECHR, 4. 3. 2008, par. 9.

that he remove his turban for inspection, despite the fact that he agreed to go through the security scanner and to be checked using a handheld detector. In addition, in accordance with the mentioned article of Protocol no. 4, he pointed out that his right to freedom of movement was violated, considering that the given security procedures should not be applied to him in the territory of the countries that are part of the European Union, given that he is a citizen of Great Britain, which was a member of the same at that time. The court concluded that security procedures at airports are necessary in order to preserve public safety, as well as that the methods of applying security measures in the mentioned case fall within the domain of free assessment of the French state, especially considering that it is a one-time measure. For this reason, this part of the petition is unfounded and, in the opinion of the court, it is necessary to reject it in accordance with Art. 35, paragraph 3 and 4 of the European Convention on Human Rights. The court also came to the conclusion that the security measures to which the passengers are subjected before boarding the plane cannot constitute a restriction of freedom of movement, and for that reason this part of the petition must also be rejected in accordance with the mentioned article.[7]

5. Examples of men using women's clothing for terrorist purposes

In contrast to the specifics of the aforementioned disputed items of clothing and certain human rights in which context we can talk primarily about the potential violation of the mentioned rights of women, when it comes to the mentioned clothing in the context of a security threat, the situation is somewhat more complex. From numerous examples, it can be concluded that this issue can be related, not only to female, but also to male perpetrators of the crime of terrorism in terms of hiding explosives, weapons or identity. There are a large number of examples in which male terrorists disguised themselves as women, both in order to escape and hide, and when carrying out the attacks themselves.

In a case that occurred in 2011, one of the leaders of the Islamic Movement for Uzbekistan, a terrorist organization that collaborated with Al Qaeda, was detained with two other associates in Kunduz, a city located in the northern part of Afghanistan. It was established that, disguised as women wearing a

[7] Phull v France, application no. 35753/03, judgment ECHR, 11.1. 2005, par. 9.

burqa, they intended to carry out suicide attacks on members of the police and other Afghan security forces (Nezavisne novine, 2011).

In 2015, seventeen Islamic State terrorists unsuccessfully tried to escape from members of the Iraqi security forces from the area around the Diyala River, i.e. the area from Baghdad to the border with Iran, using make-up and a chador (Jovanović, 2015).

During the terrorist attack that was successfully carried out by members of the Islamic State in 2017, four terrorists managed to pass the security measures of the Iranian parliament building dressed in the aforementioned women's clothing. After entering through the entrance designated for visitors, they opened fire first on the security guards, after which they continued to shoot indiscriminately in the lobby. They reached the fourth floor without any problems, where one of them blew himself up (Hrupić, 2017).

6. Conclusion

Although we should not lose sight of the other ways in which women undertake terrorist attacks, suicide bombings are among the most frequent ways of carrying them out. Accordingly, special attention is paid to the analysis of respect for religious freedoms, primarily for members of the Islamic faith, which relate to the traditional way of dressing, that is, the choice of certain items of clothing and the need for normative confrontation with potential security threats. In the search for an adequate normative approach and solution, a review was made of individual comparative law solutions, the views of the European Court of Human Rights and certain cases of misuse of women's clothing for terrorist purposes, as well as an analysis of relevant parts of the Qur'an, as a result of which we drew certain conclusions.

Although both the professional and the lay public can hear opinions that are often polarized when it comes to the right of Muslim women to wear the mentioned clothing items, it seems that it is justified to adopt a middle, compromise solution. In other words, we believe that taking a prohibitive position, that is, a position that implies a complete ban on wearing clothes that are characteristic of women of the Islamic religion, would be inappropriate. Apart from the unnecessary encroachment on human rights, it seems that an extreme point of view like this would have a counterproductive effect, which in some cases could manifest itself in the range of creating or deepening the gap between the mentioned persons and state institutions or even members of other national and religious communities, and ultimately their radicalization. On the other hand, the opposite, permissive approach, i.e. an approach

reflected in the absence of any prohibitions in this regard could lead to problems in the field of security. Although, on the one hand, accepting this position would most likely rule out potential objections related to disregard for human rights, on the other hand, such a move would create opportunities for abuse and identity concealment, not only when it comes to members of terrorist organizations, but also when it comes to male perpetrators of this crime, as evidenced by numerous cases from practice. An approach that we can label as balancing seems to be the most acceptable. In accordance with the same, we believe that the wearing of a sheila, hijab, hijab amira, khimar, and chador should be allowed in public, with the prohibition to cover the face with parts of this article of clothing. By accepting this solution, both the security criteria and the criteria regarding respect for human rights would be satisfactorily respected.

Spasojević Đorđe
Visoka škola za poslovnu ekonomiju i preduzetništvo, Beograd, Srbija

Vlajnić Jelena
Visoka škola za poslovnu ekonomiju i preduzetništvo, Beograd, Srbija

Prelević Plavšić Snežana
Visoka škola za poslovnu ekonomiju i preduzetništvo, Beograd, Srbija

SUPKULTURA ODEVANJA IZMEĐU LJUDSKIH PRAVA I TERORISTIČKE PRETNJE

APSTRAKT: Iako se na prvi pogled čini da način odevanja, predstavlja stvar potpuno slobodnog izbora svakog pojedinca, uz određene izuzetke koji se tiču poštovanja pojedinih nepisanih ili, ređe, pisanih pravila, iza kojih najčešće ne stoji nikakva ozbiljnija sankcija, postoje situacije u kojima se razmatranje navedenog pitanja podiže na znatno viši nivo. Ono se neretko dovodi u vezu sa pojedinim odevnim predmetima karakterističnim za pripadnice islamske veroispovesti, kao što su hidžab, nikab, burka i drugi. U skladu sa tim, u radu je ukazano na određene probleme koji se odnose

na pojedina pitanja koja se tiču ljudskih prava, ali i onih bezbednosnog karaktera, kojima je potrebno pristupiti ekstenzivnije, imajući u vidu i brojne primere u kojima su muškarci obučeni kao žene izvršili terorističke napade ili pobegli od nadležnih organa. U cilju predlaganja adekvatnog zakonskog rešenja, koje bi predstavljalo kompromisno rešenje koje bi uzelo u obzir potrebu za poštovanjem pomenutih prava, ali i potencijalne bezbednosne probleme, korišćeno je nekoliko metoda. Korišćen je uporedni metod prilikom sagledavanja normativnih rešenja određenih država. Primenjena je dokumentaciona analiza u pogledu presuda Evropskog suda za ljudska prava. Osim toga, analitički smo prisupili ovom problemu sagledavanjem delova Kur'ana koji se tiču odevanja i potrebe pokrivanja određenih delova tela.

Ključne reči: *ljudska prava, terorizam, teroristkinje, bezbednost, Evropski sud za ljudska prava.*

References

1. Ashni, F. Z., & Gerber, P. (2014). Burqa: Human right or human wrong? *Alternative Law Journal*, *39*(4), pp. 231–234. DOI: 10.1177/1037969X1403900406
2. Avolio, B., & del Carpio, L. (2020). Gender equality index for country regions. *International Review*, *9*(1-2), pp. 57–74. DOI: https://doi.org/10.5937/intrev2001057A
3. Alempijević, Đ., et al. (2010). *Suzbijanje trgovine ljudima – dobre prakse, priručnik za institucije* [*Combating Human Trafficking: Good Practices – A Handbook for Institutions*]. Beograd: ASTRA-Akcija protiv trgovine ljudima. Downloaded 2025, March 27 from http://repozitorijum.pravnifakultet.edu.rs/160/1/Prirucnik-za-institucije.pdf
4. Aljazeera. (2022). *Francuski senat izglasao zabranu hidžaba na sportskim takmičenjima* [*French senators vote to ban hijab in sports competitions*]. Downloaded 2025, January 10 from https://balkans.aljazeera.net/news/world/2022/1/19/francuski-senat-izglasao-zabranu-hidzaba-na-sportskim-takmicenjima
5. Bjelajac, Ž., Matijašević, J., & Dimitrijević, D. (2012). Finansiranje međunarodnog terorizma kao globalnog fenomena. *Evropsko zakonodavstvo*, *11*(39-40), pp. 384–407. Downloaded 2025, January

10 from http://repozitorijum.diplomacy.bg.ac.rs/510/1/Evropsko%20zakonodavstvo%20br.%2039-40-2012-386-409.pdf
6. Bjelajac, Ž., Tepavac, R., & Dašić D. (2012). Izvori i načini finansiranja međunarodnog terorizma [Sources and methods of international terrorism financing]. In: Bjelajac, Ž., & Zirojević Fatić, M. (ured.), *Terorizam kao globalna pretnja* [*Terrorism as a global threat*] (pp. 233–253). Novi Sad: Pravni fakultet za privredu i pravosuđe Novi Sad i Centar za bezbednosne studije Beograd. Downloaded 2025, March 25 from https://kpolisa.com/books/Terorizam_kao_globalna_pretnja.pdf
7. Chesler, P. (2010). Ban the burqa?: The argument in favor. *Middle East Quarterly*, *17*(4), pp. 33–45. Downloaded 2025, March 25 from https://www.meforum.org/middle-east-quarterly/ban-the-burqa-2777
8. Dabić, S., Spasojević, Đ., & Radulović, Z. (2023). The role of social institutions in protection of children from abuse and neglect. *Kultura polisa*, *20*(1), pp. 110–125. DOI: https://doi.org/10.51738/Kpolisa2023.20.1r.110dsr
9. Domazet, S., Marković, D., & Skakavac, T. (2024). Privacy under threat – The intersection of IoT and mass surveillance. *Pravo – teorija i praksa*, *41*(3), pp.109–124. DOI: 10.5937/ptp2403109D
10. Družetić, I. (2013). Francuska zabrana muslimanske burke i njezini odjeci u hrvatskim medijima [France's muslim burqua ban and its reflections in the croatian media]. *Studia ethnologica Croatica*, *25*(1), pp. 207–230. Downloaded 2025, January 12 from https://hrcak.srce.hr/ojs/index.php/sec/article/view/2372
11. Euronews Srbija. (2023). *Skidanje hidžaba na aerodromima u Nišu i Kraljevu: Mešihat IZ u Srbiji o diskriminaciji, Aerodromi: Pravila ista za sve* [*Removing the hijab at the airports in Niš and Kraljevo: Mešihat IZ in Serbia on discrimination, Airports: The rules are the same for everyone*]. February 21. Downloaded 2025, March 26 from https://www.euronews.rs/srbija/drustvo/78713/skidanje-hidzaba-na-aerodromima-u-nisu-i-kraljevu-mesihat-iz-u-srbiji-o-diskriminaciji-aerodromi-pravila-ista-za-sve/vest
12. Howard, E. (2012). Banning Islamic Veils – Is Gender Equality a Valid Argument?. *International Journal of iscrimination and the Law, 12*(3), pp. 147–165. DOI: https://doi.org/10.1177/1358229112464450
13. Human Rights Watch. (2009). *Beyond the burqa*. Human Rights Watch. July 2. Downloaded 2025, March 25 from https://www.hrw.org/news/2009/07/02/beyond-burqa

14. Hrupić, M. (2017). IS prvi put napao Iran: Teroristi prerušeni u žene lako su prošli sigurnosne mjere i pobili nevine [ISIS attacked Iran for the first time: Terrorists disguised as women easily passed security measures and killed innocents]. *Jutarnji list*, June 8. Downloaded 2025, January 10 from https://www.jutarnji.hr/vijesti/svijet/is-prvi-put-napao-iran-teroristi-preruseni-u-zene-lako-su-prosli-sigurnosne-mjere-i-pobili-nevine-6203441
15. Jovanović, N. (2014). Islam i savremeni svet – religijske zabrane: primeri i prakse u svakodnevnom životu [Islam and the modern world – religious prohibitions: examples and practice in everyday life]. *Religija i tolerancija*, *12*(21), pp. 161–180. Downloaded 2025, January 13 from https://ceir.co.rs/images/stories/broj_21_formular/RIT21.pdf#page=163
16. Jovanović, S. (2015). Možda je rođena s tim, a možda je terorista: Iračani uhapsili 17 isilovaca prerušenih u žene [Maybe she was born with it, or maybe she's a terrorist: Iraqis arrested 17 ISIS members disguised as women]. *Srbija danas*, March 15. Downloaded 2025, January 10 from https://www.sd.rs/clanak/mozda-je-rodena-s-tim-mozda-je-terorista-iracani-uhapsili-17-isilovaca-prerusenih-u-zene-foto
17. Korkut, B. (n.d). *Prijevod Kur'ana* [*Translation of the Qur'an*]. Downloaded 2025, January 9 from https://mizbdubica.com/wp-content/uploads/2020/06/Prijevod-Kurana.pdf
18. Kuduzović, A. (n.d.). *Kad je vrijeme za hidžab* [*When is it time for hijab*]. N-UM.COM. Downloaded 2025, May 24 from https://www.n-um.com/kad-je-vrijeme-za-hidzab-a/
19. Kurtović, A. (2018). *Zabrana nošenja vjerskih obilježja na radnom mjestu: perspektiva Suda pravde Evropske unije* [*Prohibition of wearing religious symbols in the workplace: the perspective of the Court of Justice of the European Union*]. Sarajevo: Analitika – Centar za društvena istraživanja. Downloaded 2025, January 13 from https://www.analitika.ba/bs/publikacije/zabrane-nosenja-vjerskih-obiljezja-na-radnom-mjestu-perspektiva-suda-pravde-evropske
20. deLeede, S. (2018). *Women in Jihad: A Historical Perspective*. The Hague: The International Centre for Counter-Terrorism. DOI: 10.19165/2018.2.06
21. Malešević, M. (2007). Hrišćanski identitet sekularne Evrope [Christian Identity of Secular Europe]. *Glasnik Etnografskog instituta SANU*, *55*(1), pp. 9–28. Downloaded 2025, March 24 from https://dais.sanu.ac.rs/handle/123456789/8811

22. Milošević, Z. (2012). Evropska unija i islam [The European Union and Islam]. *Srpska politička misao*, *36*(2), pp. 257–274. Downloaded 2025, January 12 from https://www.ceeol.com/search/article-detail?id=546337
23. Nezavisne novine. (2011). *Uhapšen terorista prerušen u ženu* [*Arrested terrorist disguised as a woman*]. June 28. Downloaded 2025, January 10 from https://www.nezavisne.com/novosti/svijet/Uhapsen-terorista-prerusen-u-zenu/95347
24. Okin, S. M. (1997). Is multiculturalism bad for women?. *Boston Review*, *22*(5), pp. 25–28. Dowloaded 2025, March 26 from https://www.bostonreview.net/forum/susan-moller-okin-multiculuralism-bad-women/
25. Petrović, D. (2018). O uzrocima bombaškog terorizma – ekstremna gledišta [Causes of Terrorist Bomb Attacks – an Extreme Point of View]. *Bezbednost*, *60*(2), pp. 67–85. DOI: 10.5937/bezbednost1802067P
26. Prelević Plavšić, S., Spasojević, Đ., & Dragojlović, J. (2023). Inadequacy of Application of Sentencing Policy for Perpetrators of Domestic Violence. *Kultura polisa*, *20*(3), pp. 107–127. DOI: https://doi.org/10.51738/Kpolisa2023.20.3r.107ppsd
27. Rašević, Ž., & Vlajnić, J. (2022). Novela Zakona o zabrani diskriminacije – korak napred? [Amendments to the Serbian Law on Prohibition of Discrimination: A step forward?]. *Trendovi u poslovanju*, *10*(19), pp. 109–117. DOI: 10.5937/trendpos2201101D
28. Simić, J. (2019). Burka, hidžab i nikab – gde muslimanke ne smeju da ih nose [Burqa, hijab, and niqab – where Muslim women are not allowed to wear them]. *RTS*, May 4. Downloaded 2025, January 10 from https://www.rts.rs/lat/vesti/svet/3509835/burka-hidzab-i-nikab--gde-muslimanke-ne-smeju-da-ih-nose.html
29. Spasić, D., & Vučković, G. (2011). Žene kao teroristi – Novi rodni identitet terorizma [Women as terrorists – New gender identity of terrorism]. In: Mijalković, S. (ured.), *Suprotstavljanje savremenom organizovanom kriminalu i terorizmu* [*Opposing modern organized crime and terrorism*] (pp. 259–273). Beograd: Kriminalističko-policijska akademija. Downloaded 2025, January 11 from https://jakov.kpu.edu.rs/bitstream/id/6539/1.pdf
30. Štajnver, U. (2016). Burka, čador, feredža…[Burka, chador, ferajah...]. *DW*, August 8. Downloaded 2025, January 10 from https://www.dw.com/sr/burka-%C4%8Dador-fered%C5%BEa/a-19512432
31. Vuković, I. (2018). Blasfemija i krivično pravo – uporedno zakonodavstvo i judikatura [Blasphemy and criminal law – comparative legislation and

judiciary]. *Crimen*, *9*(2), pp. 133–154. Downloaded 2025, January 13 from https://epub.ius.bg.ac.rs/index.php/crimenjournal/issue/view/41/38

32. Zedalis, D. D. (2005). Žene bombaši samoubice [Female suicide bombers]. *Bezbednost*, *47*(6), pp. 1060–1076. Downloaded 2025, January 11 from http://www.mup.gov.rs/wps/wcm/connect/d68cb4ae-3969-41b4-930f-

Anđelković M. Danijela[*]
https://orcid.org/0000-0003-2076-4721
Dimitrijević Dragomir[**]
https://orcid.org/0000-0001-8049-9451

UDK: 657(497.11)
Original scientific paper
DOI: 10.5937/ptp2502130A
Received on: February 3, 2025
Approved for publication on:
April 24, 2025
Pages: 130–142

LAW ON ACCOUNTING IN THE REPUBLIC OF SERBIA AND APPLICATION OF IAS/IFRS

ABSTRACT: In accordance with its legal accounting framework, the Republic of Serbia has adopted IAS/IFRS as the sole financial reporting framework for all entities, while taking into account certain formal specificities of medium-sized and small enterprises. The International Accounting Standards Board (IASB) played a key role in this approach. These initial observations aim to highlight the quality of financial statements as a result of the application of the current accounting legislation in the Republic of Serbia.

The issue of comparability and harmonization of financial statements is particularly relevant to medium-sized and small enterprises, as well as to companies whose securities are listed on the stock exchange. Research findings suggest that the application of the existing legal framework—specifically the mandatory and exclusive use of IFRS—has become a limiting factor in the quality of financial statements and, consequently, their representational value.

The thematic scope of this paper involves the application of a methodology based on the collection of secondary data from relevant domestic and international sources. Through processing and analysis, this information enables an assessment of the current state of financial reporting quality.

[*]PhD, Associate Professor, University Business Academy in Novi Sad, Faculty of Economics and Engineering Management, Novi Sad, Serbia, e-mail: andjelkodani@gmail.com
[**]PhD, Associate Professor, University of Kragujevac, Faculty of Economics, Kragujevac, Serbia, e-mail: dimitrijevicd@kg.ac.rs

From the perspective of financial information users—primarily investors and creditors—the second part of the paper presents research findings and proposes measures to improve accounting regulations with the aim of enhancing the quality of financial statements.

Keywords: *law on accounting, accounting regulations, financial statements, EU Directive 34.*

1. Introduction

The organization of a company's accounting function is conditioned by the applicable normative accounting regulations. Depending on who regulates and prescribes the accounting framework, it can be classified as: statutory regulations prescribed by the state or authorized state institutions; professional regulations developed and promoted by professional organizations; and internal accounting regulations created by companies (internal acts) in compliance with statutory and professional regulations. The scope of statutory accounting regulations fundamentally covers all segments of corporate accounting, with particular attention to accounting procedures and financial reporting. Statutory regulation of accounting serves as a fundamental assumption for ensuring the quality of financial statements and enhancing their informational power in line with the needs of financial information users. This highlights the importance of normative regulation in accounting. Modern statutory accounting regulations enable the accounting system to achieve a high degree of standardization, ensure the quality of financial information, and fully disclose transactions for the needs of strategic management. In other words, the accounting system, or the financial reporting system, is directly influenced by statutory accounting regulations.

The primary objective of this paper is to highlight the current level of harmonization in accounting practices and explore new trends in statutory accounting regulations that explicitly impact the quality of financial statements. Specifically, it focuses on creating financial statements that encompass both financial and key non-financial information, which define a company's growth and development. This involves formulating a new financial reporting system that complements traditional financial reporting with metrics driven by the enablers of future performance in value creation for the company. As noted by Anđelković (2020) "Information of a non-material nature from financial statements is of great importance for establishing a relationship of dependence

between customers and companies in order to create and increase the value of the firm"(pp. 43–58).

In line with the stated research objective, the hypothesis is set that there is a real need for users of information to innovate the structure of financial statements, which will comprehensively cover both the financial and non-financial perspectives of an entity's operations. This structure should be based on key success factors that include both financial information and information related to technology and innovation, customer satisfaction, and other non-financial information. The focus of the research is directed toward new, modern regulations, which result in more comprehensive financial statements aimed at increasing their quality and informative value for strategic decision-making. According to Palea (2018), a group of high-ranking experts on sustainable finance (HLEG, 2018) pointed to the need for better consideration of sustainability issues in accounting standards. All of this leads to the formulation of a financial reporting model that emphasizes the necessity of revising statutory and, consequently, professional accounting regulations.

2. The Quality Status of Financial Statements as a Result of the Application of Statutory Accounting Regulations

The organization of a company's accounting function is significantly influenced by the applicable normative framework, with the legal accounting regulations being the fundamental factor. Legal regulations essentially cover all segments of corporate accounting, with special attention focused on accounting procedures and financial reporting. In preparing financial statements, the importance of normative regulation is emphasized to ensure complete and reliable information about the economic and financial position, as well as the performance of a company, for both external and internal reporting purposes. According to the Accounting Standards Board (ASB) headquartered in the United Kingdom, as well as other regulatory accounting standards bodies, the objective of financial reporting has essentially remained unchanged. When preparing financial statements, the importance of normative regulation is emphasized to ensure complete and truthful information about the economic and financial position and the business success of enterprises for the needs of external and internal reporting. The financial statements should provide such information that offers a framework through which significant information obtained from specific sources is illustrated (Bromowich, 2001, pp. 47–72).

Financial reporting can be normatively regulated in several ways, including:

- Statutory regulations, such as the law on entities and accounting principles;
- Supplementary regulations of competent state financial institutions;
- Stock exchange rules and normative regulations concerning the exchanges issued by the government;
- Accounting guidelines and standards issued by accounting professional bodies (Alexander & Nobes, 2010, p. 48).

The international variation in the nature of legal systems often affects how accounting regulations are interpreted in different countries. National economies are characterized by basic systems related to the "Roman law codified system" and "common law" (general legal approach). In many countries, especially in Western Europe, the legal system is based on Roman law. The term "codified" is associated with this observation. Principles or postulates directly influence the definition of rules related to accounting and finance and impact the nature of regulations in a given country.

Research results indicate that the most common differences in financial reporting in a given country result from differing approaches to normative regulation in other countries regarding the law on accounting and the definition of professional accounting regulations. Similarly, different countries have varying approaches to sources of financing, tax systems, macroeconomic analyses of economic trends, and microeconomic analyses. Differences in the development of accounting practices are also evident. When it comes to the Republic of Serbia and its Accounting Laws (2013), accounting regulation is partly the result of the international environment and its regulatory body that has defined IAS/IFRS. Financial statements that are comparable with those of other enterprises are considered important instruments for protecting the interests of investors and creditors. However, it should be noted that the statutory accounting regulations in the Republic of Serbia must also reflect other environments, particularly in relation to continental European countries. Additionally, accounting regulations should take into account the specificities of the Republic of Serbia, which are reflected in its customary accounting practices. This is supported by numerous facts. One such fact relates to the country's legal and tax system. Similarly, different countries have different financial institution structures and sources of financing. Therefore, each country is inevitably faced with the fundamental question of shaping financial statements to ensure their quality and alignment with the needs and

interests of financial information users. According to the aforementioned Accounting Law (2013), information for strategic management purposes is derived from the following set of financial statements: the Balance Sheet and the Income Statement as the fundamental financial statements regarding the profitability and financial performance of enterprises; the Statement of Other Comprehensive Income; the Statement of Changes in Equity; the Cash Flow Statement; and the Notes to the Financial Statements, which are crucial for assessing the financial position and performance of enterprises. With the adoption of the Law on Accounting (2021), efforts to achieve complete harmonization of financial reporting have continued.

In the Republic of Serbia, with the adoption of the Accounting and Auditing Law (2006), further efforts were made to organize the accounting profession and achieve complete harmonization with international accounting regulations. International Accounting Standards and International Financial Reporting Standards (IAS/IFRS) represent the primary basis for the highly significant global process of harmonizing financial reporting. As noted by Dmitrović, Petković & Jakšić (2012) "The harmonization of financial reporting requires accounting to provide a more efficient understanding of the financial position of large companies (and other business entities) to ensure greater capital protection and reduce investment risk. At the global level, certain accounting rules have been established to achieve comparable financial statements" (p. 23).

When it comes to activities defining professional regulations, Barth, Landsman, Lang and Williams (2012) emphasize the influence of prominent accounting institutions worldwide, which have contributed to the global application of unified accounting rules contained in professional regulations. Based on legal provisions, our country has adopted an accounting framework that applies entirely to economic entities. The exception applies to small legal entities, which may choose not to apply IFRS if their securities are not traded on an organized securities market (Accounting and Auditing Law, 2006, Article 25). Micro-entities and entrepreneurs apply a bylaw issued by the minister responsible for financial affairs, which is based on general accounting principles. Medium-sized companies may apply IFRS that are valid for large legal entities. The aforementioned facts regarding statutory accounting regulations indicate that, in addition to the state, another highly significant guiding force in statutory regulation pertains to the accounting profession. Confirmation of this position can also be found in the new Accounting Law, more precisely in the part that regulates the issue of professional regulation (Accounting and Auditing Law, 20006, Article 2, Paragraph 4).

3. Improvement of Legal Accounting Regulations for the Purpose of Financial Report Quality

In previous discussions related to legal accounting regulations as determinants of professional regulation, the focus of the research was on traditional, classical financial statements. However, in a modern business environment, strategic management primarily focuses on strategic success measures, many of which are non-financial performance measures, such as research and development of new products, innovations, knowledge, customer satisfaction, etc. As Vunjak and Ostojić (2014) note, what is crucial from the perspective of strategic management is that "Financial reporting and operations must consider not only financial indicators but also other indicators unrelated to financial performance." Managers increasingly recognize the limited usefulness of information derived from financial statements for strategic management purposes, proposing a revision of legal accounting regulations. Palea (2018) cites Gauzès (2017), where it is stated that the "chairman of the board of the European Financial Reporting Advisory Group highlighted the need to overcome the traditional, classical approach focused on 'technical accounting.'" According to Dečman (2013) "it can be concluded that accountants are more devoted to performing traditional tasks (preparing financial statements, cost-financial control) while their involvement in planning, and especially decision-making, is less prominent" (p. 533).

A new financial reporting system for strategic management should include both financial and non-financial parameters (Škrinjar, Bosilj-Vukšić & Indihar-Štemberger, 2008, pp. 738–754). It is well known that information obtained from accounting information systems is often the basis for making business decisions. In addition to these, non-accounting information plays a particularly significant role in strategic management, as emphasized in recent years. In this context, it is necessary to explore a new approach to financial reporting for strategic management purposes. A revision of legal regulations, existing IFRS, and the broader impact of IFRS on the economy should be considered.

The revision of accounting regulations requires a preliminary approach to assessing the current state of accounting practices and previously established regulations in the field of accounting. This would contribute to defining new legal regulations that would enable the creation of comparable financial statements as a means of communication between enterprises in EU member states. Even if financial statements do not contain all the necessary information, they still provide users with a framework to compare certain

data with other sources (Kothari & Barone, 2012, p. 1). The International Federation of Accountants (IFAC) plays a key role in defining standards and postulates, which is particularly important for harmonizing accounting and financial reporting practices. If financial statements lack the necessary information, they still provide a framework for users to compare (Barone & Kothari, 2012, p. 1). The International Federation of Accountants (IFAC) plays a key role in this process by setting accounting principles and standards, thereby significantly harmonizing accounting systems and financial reporting practices. According to legal provisions in our country, the application of professional IAS/IFRS regulations does not consistently address the issue of company size or whether a company is listed on the stock exchange, particularly when it comes to the interests of small and micro-entrepreneurs regarding regulatory burdens. According to Mamić, Dečman and Sever (2015) "empirical research has confirmed that simplifying accounting regulations is justified, especially for small businesses, as it would reduce costs. At the same time, the quality of information will not be diminished due to the simplification of accounting regulations" (pp. 593–607).

Furthermore, the accounting regulatory standards in the Republic of Serbia are not harmonized with key aspects of the European Union's Directive 34. This significantly affects the quality of financial statement information in terms of comparability with the financial statements of other participants in the international market, particularly those listed on the stock exchange. According to Dragojevic, Miljevic & Milojevic, (2012) IFRS was supposed to provide a precondition for applying an explicit approach to positions from financial statements that would contribute to higher quality from the perspective of information users (p. 203).

Moreover, accounting regulations in our country have not taken into account the country's rich accounting history and, therefore, the existence of its own national accounting system. Another fundamental aspect of improving statutory and professional accounting regulations to enhance the quality of financial statements stems from modern empirical research on accounting practices. The research results indicate the need to revise the existing statutory and professional accounting regulations, to create more comprehensive financial statements that would meet the increasingly complex needs of information users for strategic management. Financial and non-financial information for strategic management purposes holds different significance depending on whether the focus is on large and medium-sized enterprises or small entrepreneurs. Statutory accounting regulations, as a prerequisite for the quality of financial statements for strategic management purposes, must

take this into account. Large, medium-sized, and small enterprises are distinct entities in terms of the organization and regulation of financial reporting. This primarily applies to external users (mainly investors and creditors). Therefore, the question arises of the extent to which small and medium-sized enterprises use such information for strategic management purposes in the context of improving their business quality. It is necessary to explore alternative performance measurement systems that would complement financial statements. To emphasize the importance of using strategic information, both financial and non-financial, accounting reports on enterprise performance should now be based on critical success factors of the enterprise. These factors should encompass not only the financial perspective but also customer satisfaction, new technologies, internal processes, and development.

The business decision-making level requires setting objectives aimed at increasing revenue sources by expanding the product range with new products and services. From the perspective of customer satisfaction, creating elements that increase their value is of primary importance. As noted by Anđelković and Vujić (2019) "Measuring customer profitability introduces another key determinant in a company's operations. This establishes a dependency and connection between factors that determine the company's operations as a result of financial performance and other factors, such as customer satisfaction, which are not financial in nature. All this contributes to increasing the company's value" (pp. 414–431).

Since customers are directly or indirectly linked to every activity that creates value for the company, the value of customer relationships should be analyzed in the same way as business operations. According to Barone & Kothari (2012) David Packard, co-founder of Hewlett-Packard, stated: "Profit is not the proper goal or purpose of management, it simply makes all other goals and purposes achievable"(p. 11). His vision emphasized that the true purpose of a business is to create value for its customers, with profit being a result of achieving that goal (Magretta, 2002, pp. 86–92). Vuković, Vukić and Sesar, (2020) further assert that "Non-financial reporting includes information on relevant measures affecting business development and results, as well as the social and environmental impact of operations. It provides essential tools for understanding development, business results, and the enterprise's position (pp. 41–58). Market and regulatory frameworks significantly influence the revision of legal regulations in modern business practices. This has led to the need for an integrated approach in creating enterprise value. The new influence on performance analysis and strategic management systems includes financial calculations alongside non-financial perspectives of the company, bringing

them into direct interdependence with finance. Cvitanović (2018) in the context of non-financial determinants that influence a company's business results, particularly emphasizes the "role of marketing and its interaction with other functions within the enterprise. The integrated approach to financial reporting also includes elements related to the intersubjective construction of value (pp. 83–94). Various strategic variables influence the measured values of financial statement information. Among the analyzed strategic variables that enhance financial indicators are research and development, innovation, knowledge, and customer satisfaction. Modern accounting regulation research demonstrates the necessity of including non-financial performance measures in financial reports. In this context, Bernard and Roland (2016) emphasize the need to reassess the current domain of finance in light of the importance of financial report information within the "new perspective of sustainable finance" (p. 441). This approach would provide a more accurate informational basis for strategic management needs. Consequently, the new approach introduces financial calculations into other dimensions of the enterprise, fostering a dialogue between these dimensions and finance. Based on the above, it can be concluded that, alongside the conventional or classical financial reporting approach supported by AISB's IAS/IFRS project. Research in this paper also highlights another system of interdependent performance measures, which stress the need for a revision of financial statement quality.

Progress linked to the aforementioned conventional financial reporting approach can be observed in one of the sets of financial statements prescribed by IAS/IFRS, which relates to "Notes to the Financial Statements" (Accounting Law, 2019). The impact of the notes is significant, as they increase the informational power of the data contained in the financial statements related to "Disclosures." In this way, users of financial statements gain a clearer picture of the financial, asset, and income position of each company. Regarding this observation, Anđelković (2020) states "The information disclosed in notes as part of financial statements, which results from the financial and non-financial performance of an enterprise, is of particular importance for objectively determining current business results, especially for making strategic decisions in the future" (pp. 46–47).

4. Conclusion

Legal accounting regulations represent a prerequisite for defining professional accounting directives and, thus, a fundamental determinant of the quality of financial reporting. The research results point to certain issues

in the application of existing legal provisions in our country. On the one hand, their application, which forms the basis of professional regulation, represents a significant regulatory burden for some enterprises in terms of their size. On the other hand, the creation of financial statements as a result of legal regulations does not account for a complex, integrated approach to information that shapes a company's financial results. This conclusion arises from the fact that our country, based on legal provisions, implemented only one area of international standards in the creation of financial statements without considering key accounting standards from other international sources. This particularly applies to Directive 34 and generally accepted accounting principles (US GAAP). Additionally, Serbia's accounting regulation did not take into account its rich accounting practice.

We believe that for the purposes of strategic management, it is necessary to supplement financial statements with alternative and mutually conditioned business performance indicators in accordance with generally accepted accounting principles (US GAAP) and the International Federation of Accountants (IFAC), which has established accounting postulates through its standards, thereby harmonizing the system for preparing and presenting financial statements. Contemporary trends indicate that International Financial Reporting Standards (IFRS) and EU directives are undoubtedly the most significant acts. This stems from the fact that most countries with professional regulations defined by the Accounting Law align their accounting rules in significant matters with these standards. In the context of financial reporting quality, it is viewed from the perspective of international accounting harmonization and, consequently, national alignment of the financial reporting system. The balanced scorecard model is a good example of an integrated performance measurement system that, among other things, serves to implement strategic intentions and predict the future. Business uncertainty and the turbulent environment in which companies operate have imposed a complex model of interrelated components in the creation of accounting reports for the needs of strategic management. Research results verify the hypothesis that strategic management will rely on financial reports which, on one hand, will encompass the financial dimension of the company's operations, and on the other hand, factors that are non-financial in nature. In this context, the concept of sustainable finance is understood as an informational support for strategic management.

Anđelković M. Danijela
Univerzitet Privredna akademija u Novom Sadu, Fakultet za ekonomiju i inženjerski menadžment u Novom Sadu, Novi Sad, Srbija

Dimitrijević Dragomir
Univerzitet u Kragujevcu, Ekonomski fakultet, Kragujevac, Srbija

ZAKON O RAČUNOVODSTVU REPUBLIKE SRBIJE I PRIMENA MRS/MSFI

APSTRAKT: Republika Srbija je u skladu sa svojom zakonskom računovodstvenom regulativom usvojila MRS/MSFI, kao jedini okvir finansijskog izveštavanja za sve subjekte, uzimajući u obzir formalne specifičnosti srednjih i malih preduzeća. Ključnu ulogu u ovakvom pristupu imao je Međunarodni odbor za računovodstvene standarde (IASB). Prethodne konstatacije imaju za cilj da ukažu na kvalitet finansijskih izveštaja kao rezultat primene postojećih zakona o računovodstvu Republike Srbije. Problem uporedivosti i harmonizacije finansijskih izveštaja naročito se odnosi na srednja i mala preduzeća, kao i na kompanije čije se hartije od vrednosti nalaze na berzi. Rezultati istraživanja ukazuju da je primena postojećih zakonskih propisa, odnosno zakonske računovodstvene regulative koja reguliše direktnu i isključivu primenu MSFI, postala ograničavajući faktor kvaliteta finansijskih izveštaja, a samim tim i njihove reprezentativne vrednostii. Tematska oblast rada definiše primenu metodologije koja se zasniva na prikupljanju sekundarnih informacija iz domaćih i međunarodnih relevantnih izvora. Kao rezultat njiihove obrade i analize dobijaju se informacije koje nam omogućavaju sagledavanje postojećeg stanja kvaliteta finansijskih izveštaja. Sa aspekta korisnika finansijskih informacija (pre svega investitora i poverilaca), u drugom delu ilustracije rada ukazuje se na rezultate istraživanja i predlog mera za unapređenje računovodstvenih propisa kako bi se poboljšao kvalitet finansijskih izveštaja.

Ključne reči: *Zakon o računovodstvu, računovodstveni propisi, finansijski izveštaji, Direktiva 34 EU.*

References

1. Alexander, D. & Nobes, C. (2010). *Finansijsko računovodstvo – međunarodni uvod* [*Financial accounting – international introduction*]. Zagreb: Mate
2. Alexander, D., Britton, A. & Jorissen, A. (2005). *International Financial Reporting and Analysis,* Second Edition, London: Thomson
3. Anđelković, D. (2020). The Significance of Financial Statements for Financial Menagement of Hotel Companies, In: *The Fifth International Scientific Conference: Tourism in function of development of the Republic of Serbia,* (pp. 43–58). University of Kragujevac: Faculty of Hotel Management and Tourism in Vrnjačka Banja
4. Anđelković, D., & Vujić, M. (2019). The Impact of Service users' satisfaction on Financialperfomance of Hotel enterprises, In: *The Fourth International Scientific Conference: Tourism in function of development of the Republic of Serbia,* (pp. 414–431). University of Kragujevac: Faculty of Hotel Management and Tourism in Vrnjačka Banja
5. Bromowich, M. (2001). The ACCA/BAA Distinguished Academic 1999 Ledture – Angels and Trolls: the ASB's Statement of Principles for Financial Reporting. *The British Accounting Review, 33*(1), pp. 47–72
6. Barone, E., & Kothari, J. (2012). *Financial accounting – international indroduction*. Beograd: Data Status
7. Barth, E. M., Landsman, R. W., Lang, M., & Williams, C. (2012). Are IFRS and US GAPP-based accounting amounts comparable? *Journal of Accounting and Economics*, *54*(1), pp. 68–93
8. Bernard, P., & Roland, P. (2016). *Finance Reconsidered: New Perspectives for a Responsible and Sustainable Finance*, Leeds: Emerald Group
9. Cvitanović, P., L. (2018). Managing accounting and financial aspects of marketing, *Journal of Accounting and Management*, *8*(2), pp. 83–94
10. Dečman, N. (2016). The use of non-accounting information in the management of a company-Croation esperiences, An Enterprise Odyssey. In: *International Conference Proceedings* (pp. 533–540). Zagreb: University of Zagreb, Fakulty of Economics and Business
11. Dmitrović, Šaponja Lj., Petković., D. & Jakšić, D. (2012). *Računovodstvo* [*Accounting*]. Subotica: Ekonomski fakultet
12. Domanović, M. B. (2010). *Balanced Scorecard – Possibilities and effects of application*. Kragujevac: Ekonomski fakultet
13. Dragojevic, D., Miljevic, T. & Milojevic, M. (2012). *New Key IFRS* International Financial Reporting Standards, *Socioeconomica – The*

Scientific Journal for Theory and Practice of Socioeconomic Development, *1*(2), pp. 201–212
14. EU Directive 34 (2013). *The EEC Official Journal*, 182/19, Brussels
15. Gauzès, J., P. (2017). Assessing the wider impact of financial reporting standards. In: *40th European accounting association annual congress* (pp. 10-12). Valencia: EFRAG
16. Mamić, S.I., Dečman, N., & Sever, I. (2015). The influence of accounting regulation simplification on the financial reporting of micro entities – the case of Croatia, *Economic Research-Ekonomska Istraživanja*, *28*(1), pp. 593–607
17. Magretta, M. (2002). Why Business Models Matter. *Harvard Business* Review, *80*(5). pp. 3–8
18. Palea, V. (2018). Financial reporting for sustainable development: Critical insights into IFRS implementation in the European, *Accoiting Forum*, *42*(3), pp. 248–260 https://doi.org/10.1016/j.accfor.2018.08.001
19. Škrinjar, R., Bosilj-Vukšić, V., & Indihar-Štemberger, M. (2008). The impact of business process orientation on financial and non-financial performance. *Business process management journal*, *14*(5), pp. 738–754
20. Zakon o računovodstvu i reviziji [Law on Accounting and Auditing], *Službeni glasnik RS*, br. 46/06, 111/09
21. Zakon o računovodstvu i reviziji [Law on Accounting], *Službeni glasnik RS*, br. 62/13. 73/19. 44/21
22. Vunjak, N., & Ostojic, S. (2011). Strategija operativnog planiranja na nivou banke [Operative planning strategy at the bank level]. *Anali Ekonomskog fakulteta u Subotici*, *47*(25), pp. 39–48
23. Vuković, R., Vukić, M. N. & Sesar, D. (2020). Non-financial reporting as part of sustainability accounting with the examples of good practices. *Journal of Accounting and Management, 10*(1), pp. 41–58

*Vasić Milica**
https://orcid.org/0000-0002-5964-3524

UDK: 342.738(4672EU+73)
Review article
DOI: 10.5937/ptp2502143V
Received on: April 2, 2025
Approved for publication on:
May 18, 2025
Pages: 143–161

THE LEGAL-REGULATORY GAP IN DATA PROTECTION BETWEEN THE EUROPEAN UNION AND THE UNITED STATES OF AMERICA – CHALLENGES AND IMPLICATIONS

ABSTRACT: In the era of global digitalization, the legal regulation of data protection has become a key challenge for international law and business. While the European Union establishes robust privacy standards through the General Data Protection Regulation (GDPR), the United States applies a fragmented approach through various federal and state laws, creating legal challenges in transatlantic data protection regulation. This paper analyzes the legal consequences of the regulatory gap between the EU and the United States, particularly in light of the annulment of the Privacy Shield agreement. Through comparative legal analysis and case studies, the paper explores how differing legal frameworks impact the global digital economy, user privacy, and international corporations. Special attention is given to the extraterritorial reach of the GDPR, its influence on U.S. legislation, and potential legal mechanisms that could contribute to regulatory harmonization. The paper highlights the need for harmonizing international data protection standards that establish a balance between legal security, privacy protection and encouraging innovation in the digital ecosystem.

*LLM, PhD Candidate and Teaching Assistant, University Business Academy in Novi Sad, Faculty of Law for Commerce and Judiciary, Novi Sad, Serbia, e-mail: milica.vasic@pravni-fakultet.info

Keywords: *GDPR, CCPA, data protection, digital society.*

1. Introduction

Data protection has become one of the key global issues in the digital era. The advancement of technology and the omnipresent connectivity via the internet have enabled the seamless flow of data across borders, creating challenges in ensuring its protection. One of the most pronounced regulatory discrepancies arises between the European Union (EU) and the United States (U.S.). Although both sides recognize the importance of data protection, their legal approaches and regulatory frameworks differ significantly.

Data protection requires specific laws that are adapted to the specific circumstances in which data are used and the risks they may pose to individuals and to the democratic order. As new risks emerge, existing regulations need to be interpreted in the light of new knowledge and, if necessary, supplemented with new regulations. The European Union has followed precisely this principle (Schwartz, 2025, p. 112). The European Union has implemented strict regulations through the General Data Protection Regulation (GDPR). This sets high standards for data collection, processing, and protection. On the other hand, the United States has adopted a fragmented approach to data protection, relying on a combination of federal and state laws and industry standards. This legal discrepancy complicates the international data flow, causes disagreements between companies and legislators, and challenges internet users. Understanding these differences is crucial for developing international data protection agreements and achieving a balance between innovation, free data flow, and the right to privacy in today's digital society.

2. Methodological Approach

The research employs a multidisciplinary methodological approach that includes the analysis of legal documents, comparative legal analysis, and case study analysis. A qualitative analysis of legal documents, including the GDPR, CCPA, and relevant court decisions, has been conducted to identify key legal norms and their impact on the regulation of digital technologies. Comparative legal analysis provides insight into the regulatory differences between the EU and the U.S., aiming to identify similarities and differences in digital privacy regulation and the potential consequences of different approaches on global legal certainty and business operations. Case studies, focusing on companies such as Facebook and Ikea, offer insights into the

legal challenges of digital privacy and the global harmonization of legal regimes.

3. Research and Analysis

The development of digital technologies brings numerous benefits but also challenges in terms of their regulation at the global level. Countries adopt different approaches to regulating data protection and privacy, leading to legal inconsistencies and creating obstacles for international business (Mirković, 2023). The European Union (EU) has taken a proactive approach to data protection through the GDPR, which requires organizations to implement privacy safeguards in advance rather than merely responding after a data breach. The key principles of the GDPR include organizational accountability, maintaining records of data processing, conducting privacy impact assessments, and, when necessary, appointing a Data Protection Officer (General Data Protection Regulation (EU) 2016/679). Additionally, the GDPR mandates the implementation of privacy concepts by design and by default, ensuring data protection integration into technological systems from the outset.

A key dilemma in data protection is extraterritorial jurisdiction: States must protect their citizens beyond their borders, but over-application of the law can lead to legal uncertainty and make global business difficult (Czerniawski & Svantesson, 2023). In that sense, one of the GDPR's key characteristics is its extraterritorial scope, meaning that its rules apply even to companies outside the EU that process data of EU citizens (General Data Protection Regulation (EU) 2016/679). For example, American companies providing digital services to European users must comply with the GDPR, even if they do not have a physical presence in Europe. To avoid hefty fines, many U.S. companies, including tech giants like Facebook, have had to adjust their business practices to align with European privacy standards.

A culture of trust is the foundation of a secure digital environment in which individuals can be confident that their data is processed lawfully, ethically, and transparently. The GDPR contributes to building this culture through strict privacy protection standards and accountability requirements for organizations that collect and process data. However, a culture of trust is not built solely through legal enforcement but also through the adoption of responsible and ethical approaches to privacy protection. The GDPR establishes rules that help organizations earn and maintain users' trust, creating a safer digital environment where personal data is protected and privacy is respected.

However, the international data transfer between the EU and the U.S. remains legally problematic. This issue was initially addressed through the Safe Harbor agreement[1] in 2000, but it was invalidated by the EU Court of Justice in 2015 in the *Schrems I*[2] case due to inadequate data protection. Subsequently, in 2016, the EU and the US established the Privacy Shield as a replacement for Safe Harbour, which established that the US provided a "substantially equivalent" level of data protection to the EU. The mechanism entered into force on 1 August 2016 (Kuner, 2017.). Subsequently, the Privacy Shield agreement was established, which was also annulled in 2020 in the *Schrems II* case. In the Schrems II case (C-311/18), the European Court of Justice invalidated the Privacy Shield in 2020, concluding that U.S. laws still did not provide adequate EU citizens' data protection. Although the agreement was an improved version of Safe Harbor, it failed to establish effective privacy protection mechanisms. At the same time, the Court upheld the use of Standard Contractual Clauses (SCCs) for data transfers but emphasized that companies must individually assess whether data can be safely transferred to the U.S., considering the level of protection available there (Data Protection Commissioner v Facebook Ireland Ltd. and Maximillian Schrems (Schrems II), 2020, C-311/18, ECLI:EU:C:2020:559).

One of the most significant factors contributing to the deep regulatory gap between the European Union and the United States in the area of data protection is the mass surveillance practices carried out by the US government. Concerns about these practices are not new, but they

[1] Safe Harbor was an agreement between the EU and the U.S., established in 2000 by a decision of the European Commission (2000/520/EC), to allow U.S. companies to self-certify compliance with EU privacy principles without requiring individual approval from regulatory authorities. It enabled U.S. companies to transfer and process the personal data of EU citizens under specific privacy protection conditions, such as transparency, limited data usage, and adequate security measures. However, it failed to provide effective data protection, which led the European Court of Justice to annul it in 2015 in the Schrems I case, stating that it did not offer sufficient guarantees against surveillance by U.S. intelligence agencies, leaving EU citizens' data exposed to mass collection without proper legal safeguards (Weiss & Archick, 2016).

[2] Schrems I (C-362/14) was a case initiated by Austrian privacy activist Maximilian Schrems, challenging the legality of transferring EU citizens' data to the U.S. via the Safe Harbor agreement. The European Court of Justice ruled that Safe Harbor did not provide adequate protection, due to the potential for surveillance by U.S. intelligence agencies and the lack of legal remedies for EU citizens. As a result of the ruling, Safe Harbor was invalidated, and in 2016, the Privacy Shield was introduced to provide a higher level of data protection in transatlantic transfers (Court of Justice of the European Union. , 2015., Maximillian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, Downloaded 2025, January 07 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CA0362#ntr1-C_2015398EN.01000501-E0001).

have intensified significantly following the revelations made public by whistleblower Edward Snowden[3] in 2013. He exposed extensive surveillance programs carried out by agencies such as the US National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ), including programs such as PRISM, XKeyscore, and Tempora. These programs allowed for the systematic collection and processing of vast amounts of communications data, often without adequate judicial oversight or notification to citizens, and often in direct collaboration with private technology companies.

The revelations caused by Snowden's disclosures have triggered a deep crisis of trust in transatlantic relations in the field of digital policy, especially in the area of the transfer of personal data. On this occasion, the European Union has re-examined whether the US legal framework ensures an "adequate" level of data protection by Article 45 of the General Data Protection Regulation (GDPR). It was precisely the existence of unlimited powers of the US intelligence services, combined with the lack of effective legal remedies for non-US persons, that was one of the key reasons why the Court of Justice of the European Union annulled the Safe Harbor and Privacy Shield mechanisms in the Schrems I and Schrems II judgments. In the Schrems II case, the Court specifically stated that the US legal system does not provide foreigners with a comparable level of protection to that within the EU, and that the legal protection mechanisms in the event of abuse by US services are neither sufficient nor efficient. This assessment primarily stems from an analysis of the surveillance programs based on the Foreign Intelligence Surveillance Act (FISA), in particular Section 702, which allows the collection of electronic communications of foreigners outside the territory of the US without a court order. Foreign Intelligence Surveillance Act – FISA) is a federal law of the United States of America that was adopted in 1978 to regulate the procedures of electronic surveillance and collection of intelligence data related to foreign powers and their agents. FISA was originally enacted to establish a legal framework and oversight mechanism

[3] Edward Snowden is a former employee of the US National Security Agency (NSA) who, in 2013, disclosed classified information about the scope and nature of mass surveillance programs carried out by US intelligence services, including programs such as PRISM and XKeyscore. His revelations were first published in media such as The Guardian and The Washington Post, and the leaked documents indicated that US agencies were systematically collecting data on the electronic communications of millions of people worldwide, including EU citizens. After that, Snowden fled the US and was granted asylum in Russia. His findings have significantly influenced the global debate on the right to privacy, surveillance, and transatlantic data protection. (Encyclopaedia Britannica. (n.d.))

for activities involving foreign intelligence targets while respecting the rights of U.S. citizens. The FISA Amendments Act of 2008 introduced Section 702, a significant expansion of the powers of US intelligence agencies. The passage of Section 702 enabled the collection of electronic communications of foreigners located outside US territory without an individual court order. It means that the data can be collected directly from the Internet service provider or through the global Internet infrastructure. Therefore, it is not necessary to show reasonable suspicion or seek approval for a specific person; rather, mass programs such as PRISM and UPSTREAM (disclosed by Edward Snowden in 2013) are sufficient (Federal Bureau of Investigation, (n.d.)).

Section 702 of the Foreign Intelligence Surveillance Act (FISA), enacted in the United States of America, represents one of the most controversial elements in the analysis of the adequacy of data protection in the context of transfers from the EU to the USA. This one provision was introduced through amendments under the FISA Amendments Act of 2008. year, enables American intelligence agencies, primarily the National Security Agency (NSA), to collect electronic communications of foreigners who are outside the territory of the USA, without having to obtain it individual court order. The practice is based on the fact that the US services may target "non-US persons" abroad for the collection of intelligence data of importance for national security. Although approval is formally requested by the secret FISA court (Foreign Intelligence Surveillance Court – FISC), that approval does not refer to specific individuals but rather to general program and procedural guidelines, which enable mass and non-discriminatory data collection. In practice, this means that communications, emails, calls, and other digital data that pass through U.S. infrastructure — even if only in transit — may be subject to processing.

The issue recognized by the Court of Justice of the European Union (CJEU) in the Schrems II judgment was the fact that individuals in the EU, whose data is being collected, do not have an effective legal remedy in the United States. Specifically, there is no mechanism through which an EU individual can find out whether their data has been subject to surveillance, nor any way to challenge such surveillance before an independent body.

Although, following Schrems II and negotiations between the European Commission and the U.S. government, U.S. President Joe Biden signed Executive Order 14086 on October 7, 2022, which provides for the establishment of the Data Protection Review Court (DPRC) as a key component in strengthening data protection in transatlantic relations — that

is, as the United States' response to the European Union's concerns regarding surveillance and legal protection of EU citizens. Under this executive order, the DPRC was established as an independent body that allows individuals from "qualifying countries" (including EU member states) to file complaints if they suspect they have been subjected to unlawful surveillance by U.S. intelligence agencies. The DPRC serves as the second, higher-instance body in a two-tier redress mechanism. Thus, the core concern lies not only in the scope and secrecy of surveillance programs but also in the asymmetry of rights: U.S. citizens enjoy certain constitutional protections regarding privacy, while foreigners abroad effectively do not have a comparable legal standing. This legal imbalance directly affects the assessment of adequacy under Article 45 of the GDPR, as the EU requires that individuals in third countries be provided with a level of protection that is "essentially equivalent" to that within the Union. In that context, Section 702 of the FISA remains one of the key arguments against the assumption that the United States provides adequate protection of the personal data of EU citizens, despite efforts to mitigate that impression through political and administrative measures (European Data Protection Board, 2023).

In this context, under the GDPR, the European Commission has the competence to issue adequacy decisions, i.e., to determine which third countries provide a comparable level of data protection. To date, the United States of America is not on that list, precisely because of structural differences in the legal systems, and in particular because of the broad powers of US intelligence agencies to monitor communications (European Commission, n.d.). As an interim solution, Standard Contractual Clauses (SCC) are applied in practice, but they require additional technical and organizational measures to mitigate the risks of inadequate data protection in third countries, which significantly increases the regulatory burden for companies. Unlike the EU, the U.S. does not have a unified federal data protection law. Instead, regulation is fragmented, with specific laws such as the Health Insurance Portability and Accountability Act (HIPAA) for health data and the Children's Online Privacy Protection Act (COPPA) for children's privacy protection. However, no comprehensive national law regulates data protection as a whole.

The only significant law at the state level is the California Consumer Privacy Act (CCPA), which sets high data protection standards and gives consumers greater rights over their information (California Privacy Rights and Enforcement Act of 2020). In addition to California, it is important to

mention the states of Virginia[4], Colorado[5], i Connectitut[6] that have enacted their own data protection laws. However, in relation to CCPA, the laws of these states do not provide for the establishment of an independent body for the enforcement of the law, nor do they allow for private lawsuits, which indicates a somewhat weaker mechanism for the implementation and protection of consumer rights. Although the CCPA shares similarities with the GDPR, there are key differences between them. The GDPR requires an opt-in model, meaning users must actively consent to the processing of their data, while the CCPA uses an opt-out model, allowing users to subsequently prohibit the sale of their data. Additionally, the GDPR applies to all companies processing data of EU citizens, regardless of their location, while the CCPA applies only to companies operating in California. Due to legal fragmentation, companies in the U.S. must comply with different laws across various states, resulting in increased regulatory costs and legal uncertainty. The proposed federal law, the American Data Privacy Protection Act (ADPPA) aims to establish a unified legal framework for user privacy protection in the U.S. It was introduced in 2022 but has not yet been passed. The law would impose strict regulations on the collection, processing, and storage of personal data for U.S. residents, granting them rights to access, correct, and delete their data (Tolson, 2025, Still No Federal Data Privacy Law: What Happened to the ADPPA?, March 18). The ADPPA is designed to replace the fragmented state privacy laws with a single federal framework. Meanwhile, political disagreements, particularly regarding whether the law should supersede state regulations like California's CCPA, have prevented its enactment, at least for now. Tech giants like Facebook (U.S.) and IKEA (EU) must adapt their business models to comply

[4] The Virginia Consumer Data Protection Act (VCDPA), from January 1, 2023, grants Virginia residents the right to access, correct, delete, and have portability of their data, as well as the right to opt out of targeted advertising, data sales, and profiling. The law also requires data controllers and processors to implement appropriate security measures and adhere to the Data Protection Principles (PrivacyEngine. 2023).

[5] In addition to California, other U.S. states have adopted comprehensive data protection laws. The Colorado Privacy Act (CPA), which took effect on July 1, 2023, grants Colorado residents rights such as access, correction, deletion, and portability of their data. It also allows them to opt out of targeted advertising and data sales. The CPA requires data controllers to conduct data protection assessments for high-risk processing activities and to implement principles such as data minimization and purpose specification (Colorado Attorney General, n.d.).

[6] The Connecticut Data Privacy Act (CTDPA), from July 1, 2023, provides Connecticut residents with similar rights as the previous two laws, including the right to access, correct, delete, and portability of personal data, as well as the right to opt out of targeted advertising and data sales. The CTDPA also requires data controllers to honor global opt-out signals and implement appropriate data protection measures (Consumer Privacy Act, n.d).

with GDPR in the EU while simultaneously adhering to the more flexible regulations of the U.S.. This dual compliance creates additional regulatory costs and can affect the business strategies of international companies.

Facebook, as a global social network originating in the U.S., must align its operations with GDPR but has often faced scrutiny from regulators for mishandling user data (Houser & Voss, 2018, pp. 50–51). The Irish Data Protection Commission imposed fines on Facebook for privacy violations related to unclear user consent options. Facebook has implemented various changes to comply with GDPR, including obligations regarding data access, transfer, deletion, and improving data security. Although the platform has adopted most GDPR guidelines, there remain concerns about user data privacy. The European company and global retail giant, IKEA, is required to fully comply with GDPR as it operates in the EU and collects personal data from users. This includes enabling users to access, correct, delete, and transfer their data, as well as transparent consent mechanisms for cookies and personalized advertising. While IKEA is known for applying high data protection standards, it is essential for the company to continuously comply with all new rules and inform users of their rights, enabling them to control their data related to purchases, preferences, and other services. One example of GDPR implementation in practice is the mandatory user consent for using cookies on their websites and providing an opt-out option for personalized advertising. However, the IKEA France case highlighted challenges in employee privacy protection, as the company used surveillance without employee consent, resulting in regulatory sanctions. In 2021, a French court fined this company €1 million for illegally surveilling employees and job applicants. It was found that IKEA had used private detectives and accessed police databases to gather information about its workers, including details about their bank accounts and union activities (MyRhline, 2025, Espionnage chez IKEA France: un réseau d'espionnage de la direction démasqué, March 15). The IKEA case indicates serious challenges in GDPR implementation regarding employee privacy and employer accountability. GDPR requires employers to collect and process employee data solely in a lawful, transparent, and proportionate manner, which IKEA violated through systematic surveillance without informing or obtaining employee consent.

GDPR sets high data protection standards that affect the business models of both technology and retail giants. This underscores the importance of effective enforcement of data protection regulations and indicates the need for ongoing oversight of corporate practices in processing employee data to ensure effective privacy protection by European legislation. The cases of

Facebook and IKEA demonstrate that non-compliance with these rules can lead to significant penalties and undermine the trust of users and employees. In the modern digital environment, where data is considered one of the most valuable resources, the effective implementation of GDPR becomes a necessary element of sustainable business. Companies that timely and consistently align their practices with regulations eliminate legal risks and potential penalties and build long-term user trust, which is a key factor for competitiveness in the global market. GDPR, although challenging to implement, provides a framework that ensures responsible data management, achieving a balance between business interests and rights to privacy.

After the previous data transfer mechanisms, Safe Harbor and Privacy Shield were invalidated by the EU Court of Justice, the European Commission adopted a new EU-U.S. Data Protection Framework on July 10, 2023. This framework allows U.S. companies to legally receive data from the EU, provided they are certified by the U.S. Department of Commerce and adhere to enhanced privacy protection standards. Key innovations include restrictions on U.S. intelligence agencies' access to collected data, thereby reducing the risks of unauthorized surveillance, the establishment of a Data Protection Review Court, which provides EU citizens with a legal mechanism to protect their rights in cases of unlawful data processing, and stricter obligations for U.S. companies, which must now comply with more precisely defined standards regarding the processing and storage of European user data. Although the framework represents progress, legal uncertainty remains, as the EU Court of Justice could potentially invalidate this agreement in the future, similar to its actions with previous solutions (Batlle & van Waeyenberge, 2024).

4. Discussion: Challenges and Perspectives of Global Data Protection Regulation

Although the official rationale for the adoption of the GDPR was to harmonize the legislation of EU member states and strengthen individuals' control over their data, this regulation also aims to level the playing field for all technology companies (Houser & Voss, 2018). GDPR initially appears as a set of restrictive rules, but in reality, it provides a framework that enables companies to enhance their operations while simultaneously increasing user trust through privacy and data protection (Pit, 2024). By introducing high privacy standards, the GDPR not only protects consumers but also contributes to strengthening trust and the competitive advantage of European companies.

However, differences in the implementation of digital regulations across countries create legal uncertainty and hinder international transactions, particularly in areas of digital data management and privacy (European Company Lawyers Association, 2023).

National legislations still exhibit significant variations in the degree of implementation of digital regulations. This may undermine the effectiveness of international transactions and reduce legal certainty, especially in the fields of privacy protection and digital asset management, where legal frameworks and technologies often develop at different paces (Stojšić Dabetić & Mirković, 2024). Additionally, the lack of global harmonization allows companies to register their businesses in jurisdictions with more lenient laws to avoid strict regulations. This complicates law enforcement on an international level and highlights the need for regulatory alignment to ensure trust in the global digital economy. Through the GDPR, the European Union insists on preserving privacy as a fundamental human right and promotes digital solidarity through fair data use and the development of technologies that enhance privacy protection (European Data Protection Supervisor, 2020).

US companies such as Google and Facebook have gained a significant market advantage thanks to weaker privacy regulations in the US. The EU, through the extraterritorial application of the GDPR, is seeking to limit this advantage and enable fair competition for European technology companies. The fundamental differences in the regulations stem from different legal and philosophical approaches – in the EU, privacy is a fundamental right, while in the US, a commercial approach prevails. Edward Snowden's revelations about mass surveillance further influenced the collapse of the Safe Harbor mechanism and encouraged the EU to strengthen regulation and impose stricter standards on entities outside its territory. In this context, US companies must adapt their operations to European standards or risk losing access to the EU market.

The implementation of GDPR requires significant financial resources, both for technical and legal compliance. Companies like Meta (Facebook) have allocated billions of dollars to adapt their systems to comply with the new regulations. The European Data Protection Board (EDPB) imposed a record €1.2 billion fine on Meta (Facebook) for the illegal transfer of user data from the EU to the U.S. The decision was the result of an investigation by the Irish Data Protection Commission (IE DPA), which found that Meta had failed to align its practices with European regulations following the Schrems II ruling in 2020. Meta relied on Standard Contractual Clauses (SCCs) as the legal basis for data transfers, but European authorities determined that

this mechanism did not provide sufficient protection against U.S. intelligence agencies. The EDPB emphasized that the data transfers were systematic, repetitive, and continuous, exposing millions of European users to potential risks. In addition to the financial penalty, Meta was given a six-month deadline to cease illegal data transfers and align its operations with Chapter V of the GDPR, which governs international data transfers. This decision is part of a broader regulatory crackdown on tech companies operating in the EU, aimed at ensuring stronger user privacy protection and stricter GDPR enforcement. The case highlights the ongoing legal conflicts between the EU and the U.S. regarding data privacy. With the Privacy Shield agreement no longer in place, companies like Meta must find a new legal basis for processing and transferring data, further complicating global digital flows. GDPR mandates that data be encrypted and anonymized, increasing costs and technical challenges for companies processing user data from the EU. While GDPR aims to protect user data, its complexity can make it difficult for individuals to understand their rights, and excessive consent requirements lead to "privacy fatigue", where users ignore terms of service due to information overload.

Although GDPR has a broad extraterritorial reach, its implementation is challenging due to regulatory differences between the EU and the U.S. While the EU insists on strict privacy standards, the U.S. legal framework is more flexible, relying on market mechanisms and industry standards. This legal uncertainty complicates business operations for global companies, which must align their business models with different regulatory environments (Swensen, 2021). On one hand, GDPR imposes strict data protection mechanisms, while the U.S. legal framework allows greater flexibility in data usage, potentially giving some companies a competitive advantage.

In this context, it is important to highlight the differences between GDPR and CCPA – two regulations that share the goal of protecting user privacy but differ in their approach and scope. GDPR, as a European law, imposes strict requirements on companies worldwide that process EU citizens' data, whereas CCPA applies to companies operating in California that meet specific criteria. GDPR requires companies to implement privacy mechanisms in advance and proactively ensure compliance with user rights. GDPR mandates explicit user consent before data collection, while CCPA allows users to request access to their data and prohibits its sale retroactively but does not impose the same level of proactive measures as GDPR. Additionally, GDPR grants users a broader range of rights, including the right to correct and delete data, whereas CCPA primarily allows users to know what information companies collect

and with whom they share it. These legal differences create challenges for global companies that must comply with both regulatory frameworks.

Beyond the fundamental differences in data protection approaches, GDPR and CCPA also differ in enforcement and penalties for non-compliance. GDPR imposes stricter fines, up to €20 million or 4% of a company's global revenue, while CCPA prescribes lower monetary penalties but allows individuals to sue if their data is improperly processed. CCPA focuses more on consumer rights concerning data sales, whereas GDPR sets comprehensive privacy standards for all aspects of personal data processing. Furthermore, GDPR requires companies to clearly define the legal basis for data processing, while CCPA does not impose the same restrictions but gives consumers more control over their data use. GDPR applies to all organizations processing EU citizens' data, regardless of location, whereas CCPA has limited jurisdiction, applying only to certain companies. These differences impact global companies that must carefully balance the requirements of both regulatory frameworks to remain legally compliant.

One of the key questions in data protection is how to reconcile different legal approaches while enabling the seamless flow of data without compromising user privacy. The EU – U.S. Data Privacy Framework represents significant progress compared to previous cross-border data transfer mechanisms but still leaves many open questions. The European Commission aimed to address the key issues that led to the annulment of the Privacy Shield, particularly regarding U.S. intelligence agencies' surveillance and legal protections for EU citizens. On the other hand, legal uncertainty remains, as it is still unclear whether the Court of Justice of the European Union (CJEU) will deem the new framework fully compliant with GDPR privacy standards.

One of the key challenges is trust in the new legal redress mechanism. The Data Protection Review Court, established under this agreement, is supposed to provide legal remedies to EU citizens if their data is compromised in the U.S. However, it remains uncertain whether this court will be independent and effective in practice. If the Data Protection Review Court remains part of the U.S. executive system, its impartiality in cases involving U.S. security agencies' interests could be questioned.

Another important aspect is the long-term sustainability of the framework. Historically, the EU and the U.S. have already unsuccessfully attempted to resolve this issue twice – first with the Safe Harbor agreement and then with the Privacy Shield, both of which were invalidated by the CJEU. If the EU-U.S. Data Privacy Framework is challenged and annulled again, it would further increase regulatory and legal costs for companies.

From the perspective of global companies, the new framework provides temporary legal certainty, allowing them to continue transatlantic data transfers without fear of sanctions or administrative barriers. However, companies investing in long-term data protection strategies face a dilemma – whether to rely on this mechanism or take additional measures.

In the context of future digital privacy regulations, the question arises whether a bilateral agreement between the EU and the U.S. is sufficient or whether a global legal framework is needed. Organizations like the OECD and the United Nations could play a key role in developing international data protection standards, which would provide a more stable legal framework for the digital economy. The gap between GDPR and U.S. legislation will remain a central issue in global privacy regulation. While the EU insists on high data protection standards, the U.S. is gradually introducing partial reforms through laws like CCPA in California, which shows a tendency to align with European principles. However, despite the current EU-U.S. Data Privacy Framework, without a comprehensive legal framework, companies will continue to face regulatory uncertainties, while end users will experience varying levels of privacy protection depending on their location. The question remains – will the world move toward global harmonization of data protection, or will we continue to witness legal fragmentation that complicates international business and privacy protection?

5. Conclusion

In the digital age, data protection represents a key challenge for international law and the digital economy. Legal discrepancies between the European Union and the United States of America create legal challenges in the cross-border transfer of information. While the EU implements uniform and strict privacy standards through the General Data Protection Regulation (GDPR), the American approach is characterized by fragmented and sector-focused regulation at the federal and state levels. This mismatch makes international data exchange difficult and creates an atmosphere of legal uncertainty for organizations that operate globally. While GDPR ensures high privacy standards and extraterritorial application of its rules, the U.S. data protection system remains inconsistent, complicating the alignment of legal regimes.

Non–classical bilateral mechanisms, such as the Privacy Shield and the new EU-U.S. Data Privacy Framework, have proven to be temporary solutions that do not guarantee long-term stability in regulating cross-border data flows. These agreements often come under legal scrutiny and risk being annulled,

highlighting the need for a more sustainable global privacy framework. The lack of comprehensive international regulations complicates the operations of multinational companies and leaves users exposed to inconsistent data protection standards. While the EU-U.S. Data Privacy Framework represents an attempt to resolve a long-standing regulatory issue, the question remains about its legal sustainability. The dilemma is whether this framework works temporarily or can endure in the long run.

A comparison of GDPR and CCPA further highlights the regulatory differences between the EU and the U.S. Although both laws share the same goal – protecting user privacy – GDPR establishes comprehensive standards applicable to all organizations processing the data of EU citizens, whereas CCPA grants greater consumer rights but within the limited jurisdiction of California. The key difference lies in the legal approach: GDPR requires proactive compliance and the application of privacy-by-design principles, while CCPA allows users to prohibit the sale of their data but does not impose the same strict obligations on companies. These differences create complex regulatory challenges for businesses operating in both markets and underscore the need for further hybridization of legal standards.

GDPR has become a global model for data protection, whereas the U.S. continues to use a fragmented approach without a unified federal law. This regulatory disparity complicates transatlantic data transfers and creates challenges for businesses and legislators. While the EU–U.S. Data Privacy Framework represents an attempt to address these issues, a long-term solution could be federal data protection law in the U.S. that aligns with European privacy standards.

It is a fact that fundamental issues of systemic oversight and legal protection are not fully resolved. The European Union continues to express reservations about the U.S. data protection system precisely because of the persistent imbalance between national security interests and individual privacy rights, significantly affecting the further regulation of data transfers between the two sides of the Atlantic.

The future of digital data regulation will depend on the international community's ability to overcome legal differences and establish a stable, comprehensive legal framework that balances privacy protection, legal certainty, and technological development. The European Union will continue to enforce high data protection standards, while the United States is increasingly introducing partial reforms through laws such as CCPA, which align with European regulations. However, without clear and harmonized legal guidelines, global companies will continue to face regulatory uncertainties, while users will experience varying levels of privacy protection depending on their location.

The lack of consistent regulation and the complexity of regulatory requirements can be just as challenging as assembling IKEA furniture without instructions – all the components are there, but without a clear guide, there is a risk of misinterpretation and failed implementation. This is precisely why a panoptic solution and the harmonization of international regulations are necessary to ensure legal certainty, privacy protection, and the promotion of innovation in the digital economy.

Vasić Milica
Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, Srbija

PRAVNO-REGULATORNI JAZ U ZAŠTITI PODATAKA IZMEĐU EVROPSKE UNIJE I SJEDINJENIH AMERIČKIH DRŽAVA – IZAZOVI I IMPLIKACIJE

APSTRAKT: U eri globalne digitalizacije pravna regulativa zaštite podataka postala je ključni izazov međunarodnog prava i poslovanja. Dok Evropska unija postavlja robustne standarde privatnosti kroz Opštu uredbu o zaštiti podataka (GDPR), Sjedinjene Američke Države primenjuju fragmentirani pristup kroz različite savezne i državne zakone, što stvara pravne izazove u transatlantskoj regulativi zaštite podataka. Rad analizira pravne posledice regulatornog raskoraka između EU i SAD-a, posebno u svetlu ukidanja *Privacy Shield* sporazuma. Kroz uporednopravnu analizu i studije slučaja, autorka istražuje kako različiti pravni okviri utiču na globalnu digitalnu ekonomiju, privatnost korisnika i međunarodne kompanije. Posebna pažnja posvećena je ulozi eksteritorijalnog dometa GDPR-a, njegovom uticaju na američko zakonodavstvo i potencijalnim pravnim mehanizmima koji bi mogli doprineti harmonizaciji regulative. Rad ističe nužnost usklađivanja međunarodnih standarda zaštite podataka koji uspostavlja ravnotežu između pravne sigurnosti, zaštite privatnosti i podsticanja inovacija u digitalnom ekosistemu.

Ključne reči: *GDPR, CCPA, zaštita podataka, digitalno društvo.*

References

1. *Adequacy decisions,* European Commission, Downloaded 2025, January 13 from https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
2. Batlle, S. & van Waeyenberge, A. (2024). EU–US data privacy framework: A first legal assessment. *European Journal of Risk Regulation*, *15*(1), pp. 191–200
3. Colorado Attorney General. (n.d.). *Colorado Privacy Act (CPA)*. Downloaded 2025, March 19 from https://coag.gov/resources/colorado-privacy-act/
4. Consumer Privacy Act. (n.d.). *Connecticut Consumer Privacy Law (CTDPA)*. Downloaded 2025, March 19 from https://www.consumerprivacyact.com/connecticut-consumer-privacy-law/
5. Czerniawski, M., & Svantesson, D. (2024). Challenges to the extraterritorial enforcement of data privacy law–EU case study. Dataskyddet, 50, pp. 127-153. Downloaded 2025, March 19 from SSRN: https://ssrn.com/abstract=4698122
6. European Commission aiming to reform GDPR enforcement rules in cross-border cases, European Company Lawyers Association, February 2023, Downloaded 2025, January 14 from https://inhouse-legal.eu/digitalisation-gdpr/european-commission-aiming-to-reform-gdpr-enforcement-rules-in-cross-border-cases/
7. European Data Protection Board. (2023). *Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework*. Downloaded 2025, March 19 from https://www.edpb.europa.eu/system/files/2023-09/edpb_opinion52023_eu-us_dpf_hr.pdf
8. Federal Bureau of Investigation. (n.d.). *Foreign Intelligence Surveillance Act (FISA) and Section 702*. U.S. Department of Justice. Downloaded 2025, March 19 from https://www.fbi.gov/how-we-investigate/intelligence/foreign-intelligence-surveillance-act-fisa-and-section-702
9. Houser, K. A., & Voss, W. G. (2018). Gdpr: The end of google and facebook or a new paradigm in data privacy? *Richmond Journal of Law & Technology*, *25*(1), pp. 1–109 Downloaded 2025, March 19 from https://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1457&context=jolt
10. Kuner, C. (2017). Reality and illusion in EU data transfer regulation post Schrems. *German Law Journal*, *18*(4), pp. 881–918

11. Mirković, P. (2023). Digital assets – a legal approach to the regulation of the new property law institute. *Pravo – teorija i praksa*, *40*(suppl), pp. 17–31 https://doi.org/10.5937/ptp2300017M
12. MyRhline (2025). *Espionnage chez IKEA France: un réseau d'espionnage de la direction démasqué*. MyRhline. Downloaded 2025, January 10 from https://myrhline.com/type-article/espionnage-ikea-france/
13. Office of the Attorney General. (2020). *California Privacy Rights and Enforcement Act of 2020*. Downloaded 2025, January 08 from https://oag.ca.gov/system/files/initiatives/pdfs/20-0009A%20%28Privacy%29.pdf
14. Pit, R. (2023). Digitalization vs. GDPR—Friends or Foes?, *Copperberg*, Downloaded 2025, January 13 from https://www.copperberg.com/digitalization-vs-gdpr-friends-or-foes/
15. PrivacyEngine. (2023). *Virginia Consumer Data Protection Act (VCDPA): A comprehensive guide*. Downloaded 2025, March 19 from https://www.privacyengine.io/blog/virginia-consumer-data-protection-act/
16. 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, Downloaded 2025, January 16 from https://eur-lex.europa.eu/eli/reg/2016/679/oj
17. Schwartz, P. M. (2025). Spiros Simitis as Data Protection Pioneer, *G.W. J. Law & Tech. (JOLT)* pp. 102-118, https://dx.doi.org/10.2139/ssrn.5146813
18. Shaping a Safer Digital Future: a New Strategy for a New Decade, European Data Protection Supervisor, 2020, Downloaded 2025, January 14 from https://www.edps.europa.eu/press-publications/publications/strategy/shaping-safer-digital-future_en
19. Stojšić Dabetić, J., & Mirković, P. (2024). Digitalna imovina – novo poglavlje u regulisanju imovinskih prava [Digital property – a new chapter in the regulation of property rights]. In: Počuča, M. (ured.), *XXI međunarodni naučni skup „Pravnički dani – Prof. dr Slavko Carić" Odgovori pravne nauke na izazove savremenog društva* [*XXI International Scientific Conference "Legal days – Prof. Slavko Carić, PhD" The responses of legal sciences to the challenges of modern society*] (pp. 667–677). Novi Sad: Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu https://doi.org/10.5937/PDSC24667S

20. Swensen, D. (2021). Data Protection v. Facebook Ireland Limited and Maximilian Schrems: Where Do We Go from Here?. *Md. J. Int'l L.*, *36*(1), pp. 24–50
21. Encyclopaedia Britannica, *Edward Snowden*. Downloaded 2025, March 19 from https://www.britannica.com/biography/Edward-Snowden
22. Tolson, B., (2025). *Still no Federal Data Privacy Law: What happened to the ADPPA?* Downloaded 2025, January 14 from https://www-smarsh.com/blog/thought-leadership/no-federal-data-privacy-law-what-happened-ADPPA
23. Weiss, M. A., & Archick, K. (2016). US-EU data privacy: from safe harbor to privacy shield. *Report prepared for Members and Committees of Congress*, 19 March 2016, Downloaded 2025, January 15 from https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/may2016/cs2016_0076.pdf

Ferati Nashit[*]
https://orcid.org/0009-0003-9140-4851

UDK: 321.011:141.7"17/18"
Review article
DOI: 10.5937/ptp2502162F
Received on: December 21, 2024
Approved for publication on:
May 5, 2025
Pages: 162–173

THE PROBLEM OF SOVEREIGNTY IN THE PHILOSOPHY OF THE 17th–18th CENTURIES
(T. HOBBES AND S. PUFENDORF)

ABSTRACT: This study presents a philosophical reflection on the question of sovereignty, viewed through a comparative analysis of two philosophers: Thomas Hobbes and Samuel Pufendorf. The field of inquiry lies between political philosophy and the philosophy of law. The literature review centers on prominent thinkers such as Machiavelli, Bodin, Spinoza, Locke, Montesquieu, Rousseau, Kant, and others, in order to provide a broader and deeper understanding of the questions surrounding sovereignty. The bibliographic research is oriented toward a comparative and analytical approach. A foundational understanding of Hobbes's and Pufendorf's philosophical positions is essential, as the comparative analysis aims to articulate their discourse on topics such as the idea of objective social unity and the ways in which national sovereignty is concretized. The comparison focuses on the form and substance of the social contract. At the core of the discussion is the relationship between popular (political) sovereignty and state sovereignty. The discourse highlights the nature of sovereign power and the issue of freedom, challenging the principle of representativeness. Positioned between the idea of indivisible force and the power to realize justice, sovereignty is situated within the conflicting contexts revealed through this comparison. The study further explores the political-legal system and the concept of the rule of law. Additionally, it addresses the

[*]PhD candidate, Religious worker, Islamic Religious Community in the Republic of North Macedonia, Tetovo, North Macedonia, e-mail: nashitferati@hotmail.com

complex relationship between internal and external sovereignty, wherein the essence of sovereignty is often compromised.

Keywords*: sovereignty, social unity, natural law, national sovereignty.*

1. Introduction

By nature, man is divided between selfishness and the need for social life. The question arises according to which objective criteria a person belongs to himself and to society at the same time. How can we strike a balance between individual freedom and social responsibility.

Under these circumstances, a sustainable social order must be created in which not only physical security is clearly stated, but also freedom, human rights for a dignified life. The means to achieve that goal is the power that rests on the parties, as the highest power. In the sense of a united society, this power was named sovereignty.

The debate about the nature of the power that governs and organizes society was early. He became the first sovereign in the 16th century (De Benoist, 1999, p. 100). In the 17th century, due to historical and political circumstances, sovereignty became one of the basic issues. Europe was in a phase of comprehensive changes and a moment of political re-examination and reorganization. The situation that followed the Thirty Years' War (1618-1648) in the political sense was a conflict for dominance (hegemony) or the balance of power between the European powers of that era. The outcome of this war was the Peace of Westphalia (1648), which divided Europe into sovereign states.

The philosophy of time requires objective arguments in conceptualizing the political and legal organization of societies. Hobbes and Pufendorf were among the first to place sovereignty as an essential part of their thinking. Three years after the Peace of Westphalia, in 1651, Hobbes publishes his famous work Leviathan, where he presents his view on sovereignty. About a decade later, Pufendorf was also involved in this discussion. The subject of the study, through a comparative analysis of two philosophers, aims to recognize the issue of sovereignty.

Sovereignty expresses the political power of society, which means that it does not derive from any other power. Being the first source makes it more absolute and unconditional than any other form of power. It legitimizes all other powers expressed by state sovereignty. State sovereignty has all the rights and mechanisms to perform the functions of sovereignty, regardless

of whether it is performed voluntarily or forcibly. In other words, society is organized within a legal order.

Referring to contemporary philosophical literature, ways of conceptualizing power are in the center of attention. It is enough to remember that sovereignty plays a fundamental role in the critical analysis of political and legal systems. Ž. Mariten, H. Arendt, M. Foucault, Đ. Agambente Hobbes and Pufendorf serve as a connecting link between antiquity, medieval theology and modern philosophy, and not only interhistorical philosophy, but also to see Nietzsche's benefit to the contemporary debate. The value of Hobbes and Pufendorf in this discourse is important for the dissertation, not only through the history of philosophy, but also to see their influence on the contemporary debate. Think of the sophisticated philosophical literature, of ways to conceptualize it at the center. It is enough to remember that sovereignty plays a fundamental role in the critical analysis of the political and legal system.

1.1. Methodology and Structure of the Paper

This paper analyzes and compares the theories of natural law of Thomas Hobbes and Samuel Pufendorf, with a focus on their views on natural law, the state of nature, and the role of the state in constituting the legal order.

To critically analyze the theories of natural law in Hobbes and Pufendorf. To identify and explain the key differences and similarities in their approaches.

To highlight the significance of their theories for contemporary debates on natural and positive law.

How do Hobbes and Pufendorf conceptualize natural law and the state of nature? In what way do their theories interpret the relationship between natural and positive law? What are the consequences of their theories for understanding the role of the state and sovereignty?

H1: Hobbes and Pufendorf develop divergent conceptions of natural law, even though they start from a similar philosophical framework of the state of nature.

H2: In Pufendorf, natural law retains its normative force even after the establishment of a political community, whereas in Hobbes it is subordinated to the absolute authority of the sovereign.

The analytical method, which will be used to interpret in detail the relevant works of Hobbes and Pufendorf, with a focus on key concepts and arguments.

The comparative method, which will be used to systematically compare their theoretical positions with the aim of identifying similarities, differences, and influence on later theories of law and the state. Introduction

Presentation of the topic, goals, research questions, hypotheses, and methodology.

Theory of Natural Law in Thomas Hobbes

- The concept of the state of nature
- Natural law and the laws of nature
- The role of the sovereign and the transformation of law into positive law.

Theory of Natural Law in Samuel Pufendorf

- The state of nature and its characteristics
- The normative force of natural law
- The relationship between natural and positive law; the function of the state

Comparative Analysis of Hobbes's and Pufendorf's Theories

- Initial premises and contextual similarities
- Key differences in the understanding of natural law, the state, and sovereignty
- Evaluation of the theoretical and practical consequences of their conceptions.

Synthesis of Key Findings in Relation to the Stated Hypotheses.

Emphasizing the significance of Hobbes and Pufendorf for contemporary legal theories, especially in the context of debates on the boundaries of natural and positive law.

Based on theoretical and comparative analysis, it is expected that the hypotheses will be confirmed:

That Hobbes reduces natural law to the instinct of self-preservation, which ultimately loses its force before the absolute authority of the sovereign.

In contrast, Pufendorf maintains natural law as a lasting moral and legal framework that remains valid even within an organized political society.

This difference has important implications for understanding the source of legal obligation and the role of the state.

2. On the concept of sovereignty

The history of mankind is so diverse that in its dynamic processes it has constantly incorporated and undermined many values and beliefs, changed the way of life and much more. What remains unchanged is the will to organize oneself. Presence in society has always required secure foundations for coexistence. Therefore, an individual in a society with all its complexity believed and accepted the power that structures (harmonizes) the mutual relations of organizations, which would not be possible without the guarantee of power. In this sense, power becomes an indispensable condition for a permanent relationship between people.

In the context of society as a whole, this power is called sovereignty. From the etymology of the term, sovereignty is a matter of power, different from other forms of power. Here, the concept of a person is at the core of the meaning of sovereignty. Instead of referring to a specific (physical) person, attention is paid to the attributes that person has, the qualities that distinguish him from the status and (superior) position of other persons. Therefore, power is a hierarchical relationship – the relationship between a person who has (exercised) power and the entity over which that power is exercised. Therefore, sovereignty cannot be understood in the usual course of society.

The power of sovereignty is the transcendental (abstract) form of society as an objective unity. The reason for sovereignty is the reason for the community, the power of the whole community is sovereignty. The abstraction of society as a single body (Hobbs, 2005, p. 109) characterizes sovereignty as the bearer of all forms of power that are expressed in society, and that is why two characteristics appear here: sovereignty is the greatest power and power is inalienable (Ruso, 2005, p. 31).

A member of society is inevitably a part of sovereignty. It is defined as part of this whole homogeneous body, which is often called civil society. The word refers to the city (civitas), the organization of society, where it may have been wrongly identified with the state (Grotius, 2007, p. 29).

First of all, there is a political understanding of society here, as a unique body, which is different from the concept of society. Within this conception, a member of society gets the status of a citizen and at this moment sovereignty is a political issue. Man, as a socio-political being, carries political power in interaction with others. For this reason, citizens constitute what Ruso called an active sovereign (Ruso, 2005, p. 31).

When talking about different levels of power, from the interpersonal to the universal structure of society, sovereignty is closely related to two basic concepts: reach and power (Fukuyama, 2013, p. 31).

The characteristics derived from the conception of society as an objective unity give it the sovereign right to exercise authority over all members of society, as well as over the territory on which it operates. Thus, a sovereign person, as Weber writes: "...holds the monopoly of the lawful use of physical force within a certain territory" (Weber, 2004, p. 142).

The concepts of legitimacy or approval, delegation, try to solve one of the central problems of sovereignty: Who deserves sovereign power? To what extent or how should force be used in conditions of superior power. The force itself does not have to be reflected, but is easily determined. What deserves attention is justice and respect for one's freedom. The question posed here refers to the philosopher B. Pascal's concern about how to "...strengthen what is right and only what is strong" (Pascal, 2005, p. 29). In this sense, sovereignty becomes a question of the principle of justice.

Formalizing transcendental power means making abstract commands or formulations of a sovereign person. In other words, the conventionalism of sovereignty is a tendency in the understanding of power. Its action is expressed in such a way that every member of society (community) is subject to the law, sovereignty (its order). Ruso defines it as a passive sovereign (Ruso, 2005, p. 31), which is formalized through the state. So, concretely, sovereignty also extends beyond the state. The concept of the nature or profile of a sovereign person gives us not only a model of state building, an expression of a political-legal regime, but also a way of governing. From this point of view, members of society acquire the status of citizen, which is different from the concept of citizen.

In terms of his internal sovereignty and omnipotence, as the only higher power, it is understood that a sovereign person enjoys absolute freedom in the exercise of power, which means that there is no power that would be his rival. The highest power is in the sense of public power, which is theoretically the last instance in the entire hierarchy of power (De Benoist, 1999, p. 100), as an inviolable, inalienable force. Therefore, it is not limited by other forms of power within society. Superiority gives absolute freedom, which implies the unlimitedness of the sovereign person (Bodin, 2007, p. 23) It is paradoxical to say that a sovereign person is limited by his order. Self-limitation is not a limitation and that is why sovereignty is legally unlimited. In this sense, a sovereign person is a moral person who is seen outside the state, outside the application of the specific law, but which is hidden in the principle and purpose of the law. The state itself as a realized act reflects the principles of sovereignty (Pufendorf, 2007, p. 75).

This optic expresses absolute strength in extension and competence. The argument is that a sovereign person can have absolute reach over the entire

territory, but should have a limited range of jurisdiction. At this moment, the question arises according to which criteria a sovereign person distances himself in terms of his competence. Again, it is troubling that the extent of a sovereign person's power remains undefined when we are in a state of unconditional sovereignty.

As regards the duties of a sovereign person as a legal person, he makes laws for his subjects, except for himself (Agamben & Sacer, 1998, p. 14). Then by what criteria does a sovereign person do justice? These questions raise concerns about finding the foundations of sovereignty and therefore determining the profile of a person with sovereign power. His task is related to the organization of the state, the way of governing, where he must create power as an expression of justice in the function of peace and social harmony.

For the sake of argument, let's consider for a moment that a sovereign person does not have absolute power. Does being non-absolute make it inexorable? As we stated above, it absolutely refers to the issue of physical (territorial) expansion as independent internal sovereignty. Also, in terms of inclusion, in terms of competence, power is absolute and inalienable. Outside this field, it is not absolute and can be placed in parallel (horizontal) power relations.

Considering the latter, Bodin, Hobbs et al. oppose this optic. They see the sovereign person as absolute in power and scope.

Thus, comprehensive, unconditional sovereignty. Sovereignty as social unity cannot be limited to individual power, community power or even the majority of society, because objective social unity is necessary and rests on any other form of power. If the other power parries the sovereignty, then it loses its essence. In this case, we will have the rule of a part, not a united society. Therefore, sovereignty is justified as a natural right of man and community. Sovereignty is the highest principle, inviolable and should not be confused with its action (state or government). This means that the state and government are the result of sovereignty and its function. This is the point of view of the school of natural law, in which all members of society without exception are members of sovereignty, that is, of a united society and an objective body.

These members operate and communicate in a defined territory. Territory has to do with property, life, housing, material possessions, etc. Territorialization is another reason for unifying and crystallizing the differences that characterize society.

In this context, the School of Natural Law is opposed to the views of the traditionalists or the Historical School, which advocate the idea that

sovereignty rests on the principle of the nation (E. Berk). For Sismond, sovereignty is the reason of the nation (Merriam, 2001, p. 42).

Nation-state sovereignty, motivated after the 30-year war (after the Peace of Westphalia in 1648), emphasized the right of nations to be sovereign.

Therefore, the unification is realized from the historical national identity, and with that unification, the sovereign right to independence and power arises. Identity and cultural basis were natural laws according to Vic's judgment (Gadamer, 2008, p. 20).

In this respect, the nation as a historical-cultural community is a dimension that differs from the idea of sovereignty abstracted in a natural sense. So, in essence, the difference is between the objectification of society on the principles of natural law and the objectification of society on the principles of historical and cultural character (Maritain, 2008, p. 28).

In the case of the Natural Law School, objective unification justifies sovereignty, despite the differences between members or groups that characterize society as a whole. On the other hand, the School of History motivates a certain (particular) expression of sovereignty, conditioned by history, tradition and culture, quite different from other societies. Power is limited by public opinion, social morality, religion or customary law, which often not only justify the source of sovereignty but also dictate and then impose the rules, laws and orders of the sovereign person (Merriam, 2001, p. 21).

However, this judgment is not about resolving the relationship between sovereignty, territory and citizenship. In terms of globalization, multicultural societies, intensive migrations, technical and economic development, the concept of classical sovereignty is called into question (Krasner, 2001, p. 229).

Territory is not only a prerequisite for the formation of a single sovereignty, but it is also a prerequisite for the limitations of this power. The geographical extent makes sovereignty a separate and powerful entity in the territory.

In this sense, sovereignty refers to a defined territory, with all competences for the exercise of its power. Outside this territory he has to deal with other rulers. It is this relationship that enables the understanding of external sovereignty. The question posed here is the nature of the relationship between internal sovereignty and external sovereignty. The most important thing in this relationship is the mutual recognition of respective sovereignties. Conventional sovereignty (Krasner, 2004, p. 2) understands the right to independence as sovereignty, not externally imposed on internal affairs.

He knows all the attributes that anyone with sovereignty must enjoy. In other words, recognition means acceptance, approval of sovereignty.

Recognition is a presumption created by diplomatic (interstate) relations and the formalization and building of relations according to a certain interest. It is known as international relations, and the plan (principles) for that relationship is known as international law. Non-recognition or limited recognition expresses an isolated, limited sovereignty and therefore cannot enjoy the rights attributed to another sovereign.

Krasner understands sovereignty as a whole in four forms of expression. The first is the sovereignty of interdependence, which is the fact that it is conditioned for interaction with other sovereigns. The second meaning has to do with the internal structure of sovereign power, that is, internal sovereignty. Sovereignty of interdependence cannot create absolute internal sovereignty.

Opposite to this (third) is Westphalian sovereignty, which advocates the absolute independence of internal sovereignty (Krasner, 2001, p. 231).

The fourth meaning is international legal sovereignty, which is based on a legal framework, where sovereign states with free relations will establish mutual relations.

If we need to define the most ideal sovereignty, then we will need "...international legal sovereignty, Westphalian (domestic) and internal sovereignty to be mutually stimulating" (Krasner, 2004, p.5) .

From this point of view, we see that sovereignty depends not only on internal factors but also on other sovereign states as a dialectical and dynamic process. Therefore, its existence depends on the existence of other sovereignties (De Benoist, 1999, p. 100). In this sense, the concept of recognition as a separate and independent state is not just a formality.

In conclusion, as discussed above, sovereignty is determined by factors:

1) Society as an absolute whole is a product of the human community and acts on this community;
2) Higher and inalienable authority (indivisible);
3) Physical expansion of the territory (territorial integrity) of internal sovereignty that structures society through state organization;
4) Recognition of sovereignty by other sovereigns, which fulfills the essential criterion regarding external sovereignty.

Beyond giving a final definition, from what we talked about, sovereignty can be understood as a transcendental (abstract) unifying power of society, the highest power within a certain territory, recognized by other sovereign states, which is absolute, free, independent, indivisible, inseparable, unlimited in matters of its jurisdiction.

Comparative Analysis: Thomas Hobbes vs. Samuel Pufendorf

Dimension	Thomas Hobbes	Samuel Pufendorf
State of Nature	War of all against all; life is "solitary, poor, nasty, brutish, and short."	A state of insecurity, but with rational norms; less chaotic than in Hobbes.
Natural Law	Instinct of self-preservation; everyone's right to do whatever is needed to survive.	Rational, universal norms prescribing duties toward oneself and others.
Laws of Nature	Rules of reason that guide toward peace, but lack binding power without authority.	Permanent rational norms valid in both natural and civil conditions.
Positive Law	Derives solely from the will of the sovereign; without sovereign, no obligation.	Builds upon natural law, which remains superior and independent.
Role of the State (Sovereign)	Absolute power of the sovereign; law is the expression of the sovereign's will.	The state institutionalizes and enforces natural law; it does not nullify it.
Source of Obligation	Obligation arises from fear and a contract transferring power to the sovereign.	Obligation comes from rationality of natural law, independent of political power.
Philosophical Basis	Mechanicism, materialism, skepticism toward natural law without authority.	Rationalism; natural law as a universal moral and rational obligation.
Purpose of Society and Law	Peace and security through absolute rule.	Balance of rights and duties in line with universal moral norms.

Source: Author's research

3. Conclusion

This work, by a comparative analysis of Hobbes' and Pufendorf's philosophy, sought to break down the questions posed by sovereignty, starting with the idea of social unityor the formation of a political society, from which state (legal) sovereignty derives; the form and conten tof the social contract; the relationship

between people's sovereignty and the sovereignty of the state; understanding the nature and properties of sovereign power; the relation of this power to free domand law, directing the discussion of the political and legal systems of the organization of society; the relationship of internal and external sovereignty. To begin with, it is in the subject's interest to create a discourse on issues of sovereignty. In addition, bibliographic research is also seen as a function of comparative analysis. Despite differing views, the common groundlies in the fact that sovereignty rests on the problem of human evil. The need to provide for life, the self ishness of human nature on the one hand, and the propensity for social life, the need for self-realization, dignity, on the other hand, putsman and society in complex, confusing and chaotic circum stances. Due to instability and great contradictions, it isneces sary to organize individual and social life on a clear and secure basis. Achieving this goal requires power that rests on the individual, but also on society it self.

Ferati Nashit
Islamska verska zajednica u Republici Severnoj Makedoniji, Tetovo, Severna Makedonija

PROBLEM SUVERENITETA U FILOZOFIJI XVII-XVIII VEKA
(T. Hobs i S. Pufendorf)

APSTRAKT: Studija je filozofsko razmišljanje o pitanjima suverenosti, viđeno kroz uporednu analizu dva filozofa: Tomasa Hobsa i Samuela Pufendorfa. Polje proučavanja leži između političke filozofije i filozofije prava. Pregled literature usredsredio se na najistaknutije filozofe poput Makijavellija, Bodena, Spinoze, Loka, Monteskjea, Rusoa, Kanta i drugih. Služi za šire i dublje prepoznavanje pitanja koja nosi suverenitet. Bibliografska istraživanja orijentisana su na komparativno analitičko proučavanje. Za ovu temu važno je osnovno znanje o Hobsovoj i Pufendorfovoj filozofskoj tezi, pri čemu uporedna analiza ima za cilj da pokaže diskurs o pitanjima kao što su ideja objektivnog društvenog jedinstva i načina konkretizacije narodnog suvereniteta. Poređenje se fokusira na oblik i sadržaj društvenog ugovora. Osnovno pitanje je odnos popularnog (političkog) suvereniteta i državnog suvereniteta. Diskurs ističe prirodu suverene moći i problem slobode, dovodeći u pitanje princip reprezentativnosti. Između ideje o nedeljivoj sili i

moći da se ostvari pravda, suverenitet se postavlja u sukobljenim situacijama koje su identifikovane prilikom poređenja. Studija ide dublje u raspravu o političko-pravnom sistemu i konceptu vladavine zakona. U drugom planu je prikazan odnos između unutrašnjeg i spoljnog suvereniteta koje je složeno pitanje, gde se suština suvereniteta često krši.

Ključne riječi: *suverenitet, društveno jedinstvo, prirodno pravo, narodni suverenitet*

References

1. Agambena, G., & Satcer, H. (1998). *Sovereign Power and Bare Life.* Stanford: Stanford University Press
2. Bodin J. (2007). *Sovraniteti* [*Sovereignty*]. Tirana: ISP & Dita 2000
3. De Benoist A. (1999). What is Sovereignty? *Telos, New York*, 9, pp. 99–118
4. Fukuyama F. (2013). *Ndërtimi i shtetit. Qeverisja dhe rendi botëror në shekullin XXI*. [*State Building. Governance and World Order in the 21st Century*]. Tiranë: AIIS
5. Gadamer H.G. (2008). *Filozofia e historisë* [*Philosophy of history*]. Tiranë: Pleiad
6. Hobbes. T. (2005). *Leviatani* [*Leviathan*]. Tiranë: IPS & Dita 2000
7. Krasner, S. (2001). Abiding Sovereignty. *International political science review*, *22*(3), pp. 229–251
8. Krasner S. (2004). *Governance failures and alternatives to Sovereignty*. Stanford, CA: Center on Democracy, Development, and The Rule of Law (CDDRL) Stanford Institute on International Studies
9. Maritain, J. (2008). *Njeriu dhe shteti*. [*Man and the State*]. Tiranë: IPS & Dita 2000
10. Merriam, C. E. (2001). *History of the Theory of Sovereignty since Rousseau*. Kitchener, Ontario: Batoche Books
11. Paskal, B. (2005). *Mendimet* [*Thoughts*]. Tiranë: Pleiad
12. Pufendorf, S. (2007). *Drejtësia si paanshmëri* [*Justice as impartiality*]. Tiranë: ISP&Dita 2000
13. Ruso. Zh. Zh. (2005). *Kontrata sociale* [*Social Contract*]. Tiranë: Botimet "Luarasi"
14. Weber, M. (2004). *Studime sociologjike* [*Sociological studies*]. Tiranë: Pleiad
15. Grotius. H. (2007). *Deti i lirë dhe Prolegamena* [*The High Seas and Prolegamena*]. Tiranë: ISP & Dita 2000

Lešanović Milica[*]
https://orcid.org/0009-0004-1954-1584

UDK: 007:004.056(497.11)
Review article
DOI: 10.5937/ptp2502174L
Received on: February 18, 2025
Approved for publication on:
May 5, 2025
Pages: 174–190

THE IMPORTANCE OF THE NATIONAL CERT INSTITUTION FOR THE REPUBLIC OF SERBIA

ABSTRACT: The National CERT is the institution responsible for coordinating, preventing, and protecting against current security risks in the information and communication systems of operators at the national level. This article explores the mechanisms of protection, prevention, and response to security threats, emphasizing the role and importance of the CERT institution for the Republic of Serbia, the application of the Law on Information Security, and the raising of public awareness about information security. Various research methods have been applied, including the method of concretization, the combined method of analysis and synthesis, the inductive-deductive method, the comparative method, and the statistical method. The Law on Information Security regulates protective measures against security risks in information and communication systems, defines the responsibilities of legal entities in managing and using such systems, and determines the competent authorities for implementing those measures. Through supervision, control, and record-keeping of all security threats in the Republic of Serbia, the National CERT enables proactive engagement by competent institutions, thereby enhancing the level of national security and Serbia's position on the global stage.

Keywords: *National CERT, information security, Law on information security, cyber threats, Republic of Serbia.*

[*]PhD student, University Business Academy in Novi Sad, Faculty of Law for Commerce and Judiciary in Novi Sad, Novi Sad, Serbia, e-mail: milica.lesan@gmail.com

1. Introductory considerations

The National Center for Prevention of Security Risks in ICT Systems of the Republic of Serbia was established within the Regulatory Agency for Electronic Communications and Postal Services, in accordance with the Law on Information Security. The primary responsibilities of the National CERT are coordination, prevention and protection against security risks in information and communication systems (ICT systems), at the national level. National CERT collects and exchanges information, informs, warns and advises persons who manage ICT systems, as well as the public of the Republic of Serbia, about possible risks. The National CERT monitors reported incidents at the national level and, based on the collected data, analyzes risks and incidents with the aim of raising awareness of the importance of information security, both among citizens, as well as among business entities and public authorities. Supervision of the work of the National CERT in the performance of tasks entrusted by this law is carried out by the Competent Authority, i.e. the Ministry of Trade, Tourism and Telecommunications (Computer Emergency Response Team [CERT], 2025).

The establishment of the National CERT represents one of the significant challenges in the modern IT world of every developed country. The establishment of the National CERT institution includes a series of activities that are reflected in the monitoring of certain activities and regulations, as well as in the provision of necessary resources. In order to establish a successful mechanism of the CERT institution at the national level, it is necessary to establish the timely action of experts through clearly defined templates for resolving incidents and dealing with emergency situations.

The importance of this article is reflected in the research of the existing mechanisms of protection, prevention and reaction to security threats, through the prism of the National CERT. Multiple research methods were applied, due to the complexity of the topic of the article, such as the combined method of analysis and synthesis, the inductive-deductive method, the comparative method, and the statistical method, as mentioned earlier. The special contribution of the article is reflected in highlighting the importance of the CERT institution for the Republic of Serbia, the current implementation of the Law on Information Security and raising citizens' awareness of information security protection.

One of the most important roles of the National CERT is its status as a clearinghouse for information on all incidents, on a statewide level. Also, its significant contribution is reflected in the development and planning of future strategies for combating threats to information systems. What makes

the capability of detailed analysis possible is that based on the annual reports of ICT system operators, experts can assess the progress of the society itself in the fight against cyber threats.

2. Challenges in the selection of personnel

In accordance with the Law on Information Security, it is necessary to follow guidelines in the preparation of documents and thus contribute to the establishment of proactive and reactive action on security incidents. The CERT team at the National CERT institution represents a group of experts in the field of cyber security, whose primary task is to respond to incidents in real time. When an incident occurs, CERT members can contribute to their company's work in determining the cause (what exactly happened) and defining specific actions to be taken to improve the situation and remediate the consequences. However, the establishment of CERT is a project that requires long-term commitment and relies heavily on a circle of international trust and cooperation with companies on a global level. Without ensuring these important attributes, the CERT establishment project may encounter numerous problems, which may have different effects on the success of achieving the main goal (Grobler & Bryk, 2016).

3. Public-private partnership and benefits of successful cooperation

The NIS directive emphasizes the importance of public and private sector cooperation, especially through public-private partnerships, in the core fight against cybercrime. This partnership is considered crucial in creating a comprehensive incident response chain, starting from the Cybercrime Center at EUROPOL, to national CERTs and internet providers in member states (Rizmal, Radunović & Krivokapić, n.d.).

The expansion of public-private partnerships in cybersecurity has become a key factor in protecting the nation's infrastructure from growing cyber threats. About 85% of critical infrastructure is owned and operated by the private sector, making their involvement in information security essential. The private sector has been engaged in the challenges and threats in the digital environment, providing software, hardware and performing functions under applicable government contracts. This way, costs for both sectors are reduced by integrating existing private and public cyber security measures, avoiding redundant and counterproductive activities (Kim, 2024).

Defining critical companies for the successful operation of the National CERT also depends on the national context of a particular country, so it is extremely important to include them in all flows and events of public importance for the community. Interested parties or key stakeholders, may include pre-existing CERTs in the country. Some of them can be CERTs established in a certain sector of the company, IT suppliers, Internet providers and large organizations with influence in the private sector. The combined collaboration, connecting with various organizations and individuals in the cyber security community, provides a comprehensive approach to incident response and threat mitigation.

4. International cooperation

The Budapest Convention on Cybercrime remains one of the primary legal frameworks for national and European legislation on cybercrime. The NIS directive also mandates the creation of a Cooperation Group to support strategic cooperation between member states, with a regular update of the work plan every 18 months. In addition, the European Union can enter into international agreements with third parties, in order to expand the scope of cooperation (Rizmal, et al., n.d.). The cooperation of all key factors is needed in order to establish a network of trust between institutions founded for the same reason – information security protection.

Difficulties at the international level that the CERT institution may encounter are problems that may arise at various levels of established international relations. A lot of effort is put into the continuity of international cooperation, and the ways in which this is achieved are being improved from year to year. The lack of effective cooperation between CERTs represents a significant risk, where risks can also be the potential unsystematic use of data and tools, as well as the lack of evaluation of existing resources (Kamara et al., 2022).

CERTs are an example of a decentralized, self-organized community of practice that encourages international cooperation in the field of cyber security (Tanczer, Brass & Carr, 2018). The ability of CERT institutions to operate across political and cultural boundaries, to build mutual trust and share technical knowledge, positions them as key players in information security management on a global scale.

5. The most common cyber security threats

One of the biggest threats at the global level is cyber warfare. The seriousness of this threat is so great that even highly developed countries would question whether they have enough resources to respond adequately, if necessary. Cyber attacks, from the most harmless to the most serious, represent a significant threat to the national security of every country. The biggest asset of their attackers is that they target critical infrastructure, financial systems and sensitive data. We are witnessing the accelerated development of digital technologies and software, so it is not surprising that nations and corporations increasingly rely on digital platforms, with a special focus on cyber security. Investments in cyber security are critical to countering the growing sophistication and dynamism of cyber criminals and their innovative methods of attack (Searchinform, 2022).

The most serious attack was recorded in 2024 when the crypto exchange Bybit suffered an attack worth as much as 1.4 billion dollars, making it the largest hacking attack in the history of the industry. A hacker took control of the exchange's wallet, resulting in the loss of funds and endangering users and company assets (CryptoAdria, 2025). It is interesting to note that the hackers responsible for the biggest cybercrime in modern history have not yet been brought to justice. After this incident, the topics of legal action by competent institutions in cooperation with IT experts and consultants in the field of cyber security were raised. Citizen petitions have been launched, which aim to make the necessary changes to the Law on Information Security, at the level of domestic and international legislation. It is necessary to influence the urgency of adopting regulations that would facilitate international cooperation and bringing to justice of the perpetrators of criminal acts, from whatever continent they operate.

6. The most common cyber security threats in the Republic of Serbia, in the period from 2020 to 2023

6.1. Report for 2020

In the report published on the official website of the National CERT of the Republic of Serbia for the year 2020, information is available on the most common types of cyber attacks in that period. Table 1 shows the five most represented groups of incidents registered in the Republic of Serbia.

Based on the information available, it was observed that the most common attacks relied on weak user passwords rather than specific system

vulnerabilities. The group of incidents that is the most dominant is the attempt to break into the ICT system (17,332,830), which includes an attempt to reveal user credentials, as well as an attempt to exploit system vulnerabilities. In second place is the group of incidents of unauthorized data collection (8,470,838), in which port scanning and social engineering are the most represented (CERT, 2020).

An example from March of this year refers to an attack on state structures, when the target of the attack were the servers of the Public Utility Company "Informatika" from Novi Sad. Hackers broke into the information system via a "fake" email, which gave them access to data and gave them the opportunity to block the city administration and prevent it from continuing to work on regular basis (Đurić, 2021).

6.2. Report for 2021

The report below provides a summary overview of cyber incidents in 2021, with an emphasis on the statistics of attack groups and incidents that occurred in ICT systems of particular importance.

In this research, attention was paid not only to threats at the given moment, but also to the importance of a strategic approach to protecting the system from such attacks in the future. In 2021, the trend of increasing malicious campaigns through fake electronic messages and links (phishing) and misuse of the circumstances of the pandemic and the impact of remote work continued. Compared to the previous year, the introduction of automation in information security is becoming more pronounced in the defense of system security and information security (CERT, 2021).

The importance of continuous monitoring and updating of necessary IT system upgrades, as well as the importance of continuous education of experts in this field, clearly indicate that a comprehensive approach of the National CERT is necessary for a successful response to modern security threats. This type of annual report and display of registered threats can be very helpful in making decisions to strengthen defense mechanisms against future attacks. In 2020, the total number of the most represented groups of incidents (25,954,294) is significantly higher than the total number of incidents in 2021 (13,261,258), which indicates that the establishment of the National CERT significantly contributed to the reduction and better response to existing incidents. From the comparative view, we conclude that in 2021, serious progress was made in modernizing access and solving security incidents, which makes the fight against security risks and threats in information technologies more advanced.

6.3. Report for 2022

From the annual report on statistical data on all incidents in the field of cyber security, it is noted that attacks on ICT systems of particular importance in 2022 were more diverse than in previous years, but certain trends were still widely represented.

The biggest number of incidents recorded in 2022 refers to a group of incidents of unauthorized data collection, among which the type of attack called port scanning is the most common (CERT, 2022). This attack aims to gather information about systems without immediate and direct damage and most often serves as preparation for further research and planning of future attacks. Another common attack in this group of incidents, is an attempt to discover user credentials, that is, attacks that rely on trying out different combinations of usernames and passwords, until a credential takeover and data misuse is established.

The example from June 2022 indicated the increased danger of the most notorious hacker attacks, such as those in developed and modern countries of the world. On this occasion, hackers successfully took over the cadastre database, causing serious difficulties in the work and preserving the credibility of data on property records in the Republic of Serbia. The consequences of this attack were reflected in difficulties in property transactions and legal affairs of citizens (Aničić, 2024). This attack triggered many events in all aspects at the state level, such as the consideration of the amendment of the Law on Information Security, with the aim of timely response to security incidents and prescribing adequate punishments for the perpetrators.

6.4. Report for 2023

The 2023 Incident Report provides a concise overview of the types of attacks that were most prevalent in ICT systems of particular importance. As the most common attack this year, the type of attack that deals with port scanning stands out. These attacks are represented on an increased scale due to the automation of processes and include ICT systems that are represented in the digital infrastructure and electronic communications (CERT, 2023).

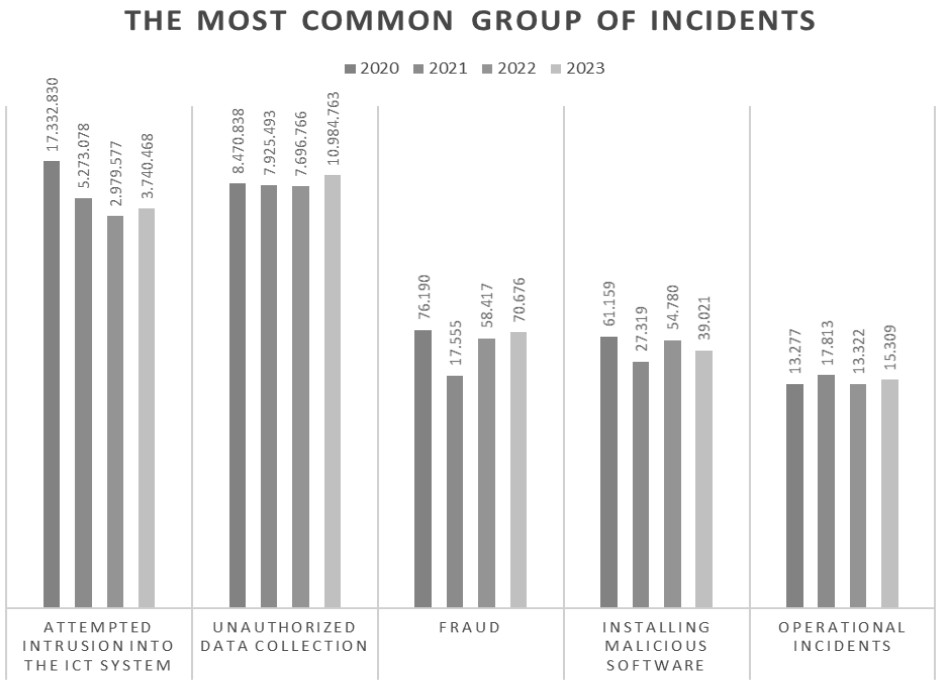
The example of the hacker attack on the Electric Power Company of Serbia, which surprised state authorities and citizens at the end of December, represented a serious security problem and an appeal to institutions to more actively deal with these security segments. Namely, the hacker group “Qilin” took responsibility for this attack, which was carried out with the aim of

extorting money by "taking over" the company's server (Vlaović, 2024). It is interesting to note that the authorities from the National CERT were not open to cooperation in informing the public about the incident at the given moment, which is not in accordance with their postulates. Transparency and work with citizens and competent institutions would increase the level of trust in the institution of the National CERT, while also facilitating the acceptance of new regulations in the planned amendments to the Law on Information Security.

It is important to note that the human factor remains the main source of risk in the information security of the Republic of Serbia. The number of security incidents at all levels is constantly increasing, the variety of groups of incidents is not negligible and requires special attention when creating strategies and defense mechanisms against future cyber threats.

6.5. Analysis

Chart 1. Presentation of the most represented groups of incidents, in the period from year 2020-2023.



Source: Author's research

By comparing data from available annual reports and monitoring trends in the total number of recorded security incidents, we can proactively respond to future threats and incidents. Using the graph shown above, we can see the trend of growth and decline in the number of registered incidents and compare it with available data for the period from 2020 to 2023. The group of attacks of attempts to break into the ICT system dominates in 2020 (13,592,362 fewer registered cases were recorded in 2023), while the group of incidents of unauthorized data collection reaches its growth peak in 2023 (2,513,925 more registered cases compared to 2020). During the entire research period, cases of malicious software installation, fraud and operational incidents were recorded, which indicates the need to plan protection mechanisms against these groups of incidents. After the publication of the annual report for 2025, we will be able to create a broader picture of the activities undertaken and analyze the level of improvement of defense mechanisms against cyber attacks.

7. Criminal acts against the security of computer data – the most common criminal acts in the Republic of Serbia

7.1. Unauthorized access to a protected computer, computer network and electronic data processing

On the basis of Article 302 of the Criminal Code, measures of protection and responsibility of perpetrators of criminal acts, due to violations of the regulations provided for in the document, are prescribed. The law stipulates that any person who has unauthorized access to a computer or computer network will be punished with a fine or imprisonment for up to 6 months (Criminal Code, 2005, Art. 302). In the previous analysis of the most common crimes against the security of computer networks in the Republic of Serbia, based on publicly available reports of the National CERT, we concluded that this is one of the most common crimes. It should be pointed out that it is often difficult to detect the perpetrator and hold him accountable for the crime, while the prescribed "mild" punishment leaves room for the perpetrator's recovery. Perpetrators can be punished with a prison sentence of up to 3 years, in the event that more serious consequences have occurred (disruption of the network's functioning or serious system downtime, for example). We should remember examples from the world where the material benefit is so great that it motivates the perpetrator to engage in illegal activities, and in case he is caught, the benefit is much greater than the defined sanctions.

7.2. Computer fraud

When it comes to the criminal offense of computer fraud (Criminal Code, 2005, Art. 301), it is necessary to point out the financial aspect in punishing the perpetrators, where the perpetrator in this case is punished more severely, because the goal is to acquire (most often significant) illegal property benefits. The range from four hundred and fifty thousand dinars to over one million and five hundred thousand dinars indicates the seriousness of these crimes and the prison sentence of up to 10 years.

In the examples discussed in the previous part, the process was mostly conducted against an unknown perpetrator, in cases where there was significant material damage. Namely, mostly the perpetrators who are charged with the most serious crimes against the security of computer data, are members of organized criminal groups, "operate" from various locations in the world and are practically uncatchable. One of CERT's tasks is to collect relevant information on computer fraud crimes, among others, as well as planning future protection mechanisms and legal regulation.

7.3. Computer sabotage

When we talk about computer sabotage, the Law prescribes that any person who enters, destroys, deletes, changes, damages, conceals or otherwise renders computer data or programs unusable or destroys or damages a computer or other device for electronic processing and data transmission (Criminal Code, 2005, Art. 299), it is necessary to analyze the motive for such illegal action in depth. Perpetrators can be employed in a certain company, which is of national importance, in the event that they misuse and manipulate data of state importance, they can be punished with imprisonment from six months to five years. The perpetrators of this criminal act may have different intentions, from obtaining illegal benefits (as in the cases we dealt with in the analysis), or even problematic behavior of employees within the company (risk of inadequate personnel). On the example of the National CERT, a risk of incredible proportions would follow in the event that an employee of this institution commits a criminal act, similar to this one, considering that the data that the authorities in the CERT have are usually (strictly) confidential.

7.4. Creating and introducing computer viruses

An unavoidable topic in the cyber world and the cyber space of the Republic of Serbia are various computer viruses and fake emails that contain links to such programs. The reason for the creation of computer viruses and their distribution is widespread among world hackers, because it represents a way to manipulate data and files on the "infected computer". In the Republic of Serbia, a fine or a prison sentence of 6 months to two years, depending on the seriousness of the crime (Criminal Code, 2005, Art. 300), is prescribed for the execution of this criminal offense. We have witnessed that in the modern world of digital technologies and the constant improvement of the hacking abilities of the perpetrators, the questioning of the adequacy of the punishment for this crime will be a potential item in the coming period. Amendments to the Law envisage the improvement of measures and sanctions for perpetrators in accordance with current statistical data on crimes committed in the Republic of Serbia.

8. Positive and negative aspects of the implementation of the Law on Information Security in the Republic of Serbia

The Law on Information Security in the Republic of Serbia represents a significant step in the direction of harmonization with European standards. This Law more closely regulates the necessary protection measures against security risks in ICT systems, considers and prescribes the responsibilities of legal entities in the management and use of information and communication systems, and determines the competent authorities for the implementation of prescribed protection measures.

The negative aspect of the adopted Law on Information Security is reflected in the fact that it does not provide enough transparency regarding key data on ICT systems of particular importance. The idea that the entire records of ICT operators of special importance should be secret may seem like an excessive measure, however, it is necessary to make specific technical information publicly unavailable, in order to prevent misuse.

The establishment of the Information Security Office (ISO), which would include the National CERT, raises a number of questions related to political influence, transparency and available professional capacities. It is recommended that ISO must publish annual reports containing analyzes of the most significant incidents (like the National CERT), which would help monitor security trends over a longer period of time (Ministry of Innovation and Technological Development [MIT], 2023).

In the long term, the Law on Information Security should provide more effective supervision over the implementation of security regulations, over the work of the National CERT, special CERTs and private companies, because the current supervision system did not show the necessary level to achieve the desired results. Cooperation with key institutions, clearly defined consequences of unwanted criminal acts, the expertise of personnel and the developed awareness of citizens about potential security threats can also contribute to the effective implementation of the Law on Information Security.

We pay special attention to certain articles of the Law on Information Security, because they concern the National CERT and the powers that are defined and stipulated. The Law on Information Security envisages an important role for this institution in the coordination and protection of ICT systems in Serbia, as well as in the exchange of information on security risks and security incidents. National CERT is authorized to perform defined activities, including monitoring security incidents, providing early warnings, advising ICT system operators, as well as working to raise awareness among citizens and private organizations about the importance of information security (Information Security Law, 2016, Art. 15).

The National CERT is also responsible for establishing coordination with other CERTs in Serbia, as well as with similar organizations abroad, in order to ensure an effective response to incidents and exchange of information. Nowadays, it is necessary, through cooperation with domestic and foreign institutions (state and private), to establish the possibility of anticipating future incidents, using pre-tested response patterns and predictions based on past events. Also, the Law on Information Security stipulates the obligation to hold regular meetings between different CERTs in Serbia, in order to exchange information and coordinate activities related to the security of ICT systems (Information Security Law, 2016, Art. 15a).

The law provides for the supervision of the work of the National CERT, which is carried out by the competent authority, in order to ensure compliance with the predefined activities. Oversight is necessary to verify that CERT has adequate resources and responds in a timely manner, in the event of a security incident. The supervision of the work of this institution is of great importance, it enables transparency over the work of CERT and the use of resources, it allows citizens to have an insight into the results achieved by the National CERT and, perhaps most importantly, whether it fulfilled what was expected of it.

Independent operators of ICT systems are obliged to form their own CERTs, which perform tasks prescribed by internal acts, from the

development of Procedures, Regulations, Plans, to mandatory employee training (Information Security Law, 2016, Art. 19).

The Law on Information Security was adopted in order to improve the ICT system protection system in Serbia. National CERT was created for the same reason. It is inevitable that the existing Law on Information Security needs to be amended (the amendment is planned), but considering that CERT was only recently established in the Republic of Serbia, many activities are largely covered by the Law on Information Security.

9. Concluding considerations

The National CERT (Computer Emergency Response Team) institution for responding to computer incidents in the Republic of Serbia plays a key role in protecting information systems and preventing cyber threats at the national level. National CERT's mission is accomplished by coordinating cyber attack response activities, gathering and sharing information about security incidents, and providing timely guidance and notifications. Providing support to both state and private organizations is one of the basic tasks of the National CERT.

The aim and importance of this article is reflected in the research of the mechanisms of protection, prevention and reaction to security threats, with an emphasis on the importance of the CERT institution for the Republic of Serbia, the application of the Law on Information Security and raising the awareness of citizens on the protection of information security. The importance of this article is also reflected in the research of the existing mechanisms of protection, prevention and reaction to security threats, through the prism of the National CERT.

The organizational structure of the National CERT includes cooperation with similar security centers in the country and abroad, which enables efficient and timely exchange of critical information at all levels. It is important to note that the effectiveness of the National CERT may depend on several factors, including employee education, standardization of security incident management mechanisms, and cooperation with private and international partners and organizations. It is necessary to provide a sufficient number of experts, with the active participation of all employees in the company, in order to respond to potential threats and establish complete protection of information and information systems. The Law on Information Security of the Republic of Serbia lays the foundation for the efficient work of the National CERT institution, and its implementation enables activities to be harmonized with European and international standards.

The reports of the National CERT of the Republic of Serbia in the period from 2020 to 2023 provide a concise overview of the evolution of registered cyber threats, with an emphasis on different types of attacks and trends that developed during those years. In 2020, the COVID-19 pandemic led to a significant increase in the number of attacks, especially on weak user passwords and access via VPN, which has become common due to the conduct of business activities from home. Phishing attacks, as well as attacks on user credentials, were among the most prevalent in 2021, while in 2022, the attacks became more diverse, but the key trends remained unchanged. In 2023, attacks via fake e-mails and links, especially in healthcare, banking and online commerce, were also in focus.

Although the Law on Information Security has given the necessary attention to the CERT institution, it is important to emphasize that the legislative framework should enable not only technical security, but through transparency, also influence the raising of citizens' awareness of security incidents. Preservation of data confidentiality is an indispensable item in the Law on Information Security, while open communication and incident reporting would be essential to create long-term trust in the institution of the National CERT, as well as to improve the reaction and preparedness of all actors to future threats.

Effective oversight of the work of the National CERT and the private sector can help in preventive actions and responses to cyber attacks, as well as in the formation and implementation of harmonized legal frameworks to ensure accountability of all actors. Cooperation with relevant competent institutions and clear definition of legal consequences are key factors in maintaining security in information systems. Personnel training within the institution of the National CERT, political independence of the institution from possible external influences, are key to creating an effective system of protection against security threats in the Republic of Serbia.

Lešanović Milica
Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, Srbija

ZNAČAJ INSTITUCIJE NACIONALNOG CERT-A ZA REPUBLIKU SRBIJU

APSTRAKT: Nacionalni CERT je institucija koja se bavi koordinacijom, prevencijom i zaštitom od aktuelnih bezbednosnih rizika u informaciono-komunikacionim sistemima operatora, na nacionalnom nivou. Značaj ovog članka ogleda se u istraživanju mehanizama zaštite, prevencije i reakcije na bezbednosne pretnje, sa akcentom na važnosti institucije CERT za Republiku Srbiju, primeni Zakona o informacionoj bezbednosti i podizanju svesti građana o zaštiti informacione bezbednosti. Primenjene su određene metode istraživanja, kao što su kombinovana metoda analize i sinteze, metoda konkretizacije, induktivno-deduktivna metoda, uporedna metoda i statistička metoda, između ostalih. Zakonom o informacionoj bezbednosti uređuju se mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornosti pravnih lica prilikom upravljanja i korišćenja informaciono-komunikacionih sistema i određuju se nadležni organi za sprovođenje mera zaštite. Nacionalni CERT kroz nadzor, kontrolu i evidenciju svih bezbednosnih pretnji u Republici Srbiji, omogućava proaktivno delovanje nadležnih institucija, koje doprinose poboljšanju nivoa bezbednosnosti i položaju Republike Srbije na globalnom nivou.

Ključne reči: *Nacionalni CERT, informaciona bezbednost, Zakon o informacionoj bezbednosti, cyber pretnje, Republika Srbija.*

References

1. Aničić G. (2024). Pregled najvećih Cyber napada u Srbiji: Bezbednost na testu poslednjih 5 godina [Overview of the biggest cyber attacks in Serbia: Security on the test for the last 5 years]. *FTN Informatika*. Downloaded 2025, February 1, from https://ftninformatika.com/pregled-najvecih-cyber-napada-u-srbiji-bezbednost-na-testu-poslednjih-5-godina/

2. CryptoAdria Portal (2025). „Najveći kripto hakerski napad u istoriji“: Bybit eksploatacija je najnoviji sigurnosni udarac za industriju [“Biggest crypto hack in history”: Bybit exploit is the latest security blow to the industry]. *CryptoAdria Portal*. Downloaded 2025, February 1, from https://cryptoadria.com/portal/2025/02/24/najveci-kripto-hakerski-napad-u-istoriji-bybit-eksploatacija-je-najnoviji-sigurnosni-udarac-za-industriju/
3. Đurić, J. (2021). U Srbiji najčešći sajber napadi „pecanjem“, hakeri traže žrtve putem aplikacija i linkova [In Serbia, the most common cyber attacks are “phishing”, hackers look for victims through applications and links]. *Euronews Serbia*. Downloaded 2025, February 1, from https://www.euronews.rs/magazin/tehnologija/4211/u-srbiji-najcesci-sajber-napadi-pecanjem-hakeri-traze-zrtve-putem-aplikacija-i-linkova/vest
4. Grobler, M., & Bryk, H. (2010). Common challenges faced during the establishment of a CSIRT. *2010 Information Security for South Africa*, pp. 1–6. https://doi.org/10.1109/ISSA.2010.5588307
5. Kamara, I., van den Boom, J., Stuurman, K., van Brakel, R., Leenes, R., Auwema, N., Duijnhoven, H., Kassim, S. R. B. M., Shamsuddin, S. B., Li, S., & Arief, B. (2022). How national CSIRTs operate: Personal observations and opinions from MyCERT. In *2022 IEEE Conference on Dependable and Secure Computing (DSC)* (pp. 1–2). IEEE. https://doi.org/10.1109/DSC54232.2022.9888803
6. Kim, R. (2022). Public-private partnerships in national cybersecurity. *Michigan Technology Law Review*. Downloaded 2025, February 1, from https://mttlr.org/2022/01/public-private-partnerships-in-national-cybersecurity/
7. Krivični zakonik [Criminal Code]. *Službeni glasnik RS*, br. 85/05, 88/05 – ispr., 107/05 – ispr., 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19 i 94/24
8. Ministry of Innovation and Technological Development, & SHARE Foundation. (2023). *Komentari SHARE Fondacije na Nacrt zakona o informacionoj bezbednosti i Obrazloženje Zakona o informacionoj bezbednosti.* [*SHARE Foundation›s Comments on the Draft Law on Information Security and the Explanatory Memorandum to the Law on Information Security*]. Downloaded 2025, February 1, from https://mit.gov.rs/extfile/sr/6891/Obrazlozenje%20ZIB.pdf
9. Nacionalni CERT Republike Srbije. (2025). [National CERT of Republic of Serbia]. *O Nacionalnom CERT-u.* [*About National CERT*]. Downloaded 2025, February 1, from https://www.cert.rs/rs/stranica/57-O+Nacionalnom+CERT-u.html

10. Nacionalni CERT Republike Srbije. (2020). [National CERT of Republic of Serbia]. *Izveštaj o statističkim podacima za 2020. godinu.* [*Report on statistical data in 2020*], pp. 25–27. Downloaded 2025, February 1, from https://www.cert.rs/files/shares/Izve%C5%A1taj%20o%20statisti%C4%8Dkim%20podacima%20za%202020.%20godine.pdf
11. Nacionalni CERT Republike Srbije. (2021). [National CERT of Republic of Serbia]. *Izveštaj o statističkim podacima za 2021. godinu.* [*Report on statistical data in 2021*], pp. 43–46. Downloaded 2025, February 1, from https://www.cert.rs/files/shares/Izvestaj%20o%20statisti%C4%8Dkim%20podacima%20za%202021%20godinu.pdf
12. Nacionalni CERT Republike Srbije. (2022). [National CERT of Republic of Serbia]. *Izveštaj o statističkim podacima za 2022. godinu.* [*Report on statistical data in 2022*], pp. 40–43. Downloaded 2025, February 1, from https://www.cert.rs/files/shares/Izvestaj%20o%20statisti%C4%8Dkim%20podacima%20 za%202022.%20godinu.pdf
13. Nacionalni CERT Republike Srbije. (2023). [National CERT of Republic of Serbia]. *Izveštaj o statističkim podacima za 2023. godinu.* [*Report on statistical data in 2023*], pp. 43–46. Downloaded 2025, February 1, from http://skr.rs/z0DM
14. Zakon o informacionoj bezbednosti [Information security law], *Službeni glasnik RS*, br. 6/16, 94/17 i 77/19
15. Rizmal, I., Radunović, V., & Krivokapić, Đ. (n.d.). *Vodič kroz informacionu bezbednost u Republici Srbiji* [*A guide to information security in the Republic of Serbia*]. Centar za evroatlantske studije – CEAS i Misija OEBS-a u Srbiji. Downloaded 2025, February 1, from https://www.osce.org/files/f/documents/b/b/272206.pdf
16. SearchInform. (2022). Cyber threats to national security. *SearchInform Blog*. Downloaded 2025, February 1, from https://searchinform.com/blog/2022/11/18/cyber-threats-to-national-security/
17. Tanczer, L. M., Brass, I., & Carr, M. (2018). CSIRTs and global cybersecurity: How technical experts support science diplomacy. *Global Policy, 9(*1), pp. 60–66. https://doi.org/10.1111/1758-5899.12625
18. Vlaović, G. (2024). Hakerski napad na EPS: Šta se zna o grupi „Qilin" koja ga je izvela, ali i o starijim protokolima u preduzeću? [Hacking attack on EPS: What is known about the "Qilin" group that carried it out, but also about the older protocols in the enterprise?]. *Danas.* Downloaded 2025, February 1, from https://www.danas.rs/vesti/ekonomija/hakerski-napad-eps-qilin/

INSTRUCTIONS TO AUTHORS

FOR WRITING AND PREPARING MANUSCRIPTS

The editorial board of the journal "Law – Theory and Practice" requests that authors submit their texts for publication in accordance with the following instructions.

The journal publishes texts in the fields of law, economics, and social sciences. The journal accepts scientific articles, reviews, critical analyses, regulatory analyses, commentaries on court decisions, student papers, and other contributions. Texts should be submitted in both English and Serbian via the online OJS platform.

(http://casopis.pravni-fakultet.edu.rs/index.php/ltp/about/submissions).

The accepted papers will be published in English.

All submitted texts are subject to review. Each scientific paper is reviewed by a minimum of two reviewers selected by the editorial board.

The editorial board reserves the right to adjust the text to the journal's editorial standards.

General Information for Writing Papers:

The submitted text must be written in Microsoft Word, using the Times New Roman font, size 12 pt, in Latin script, with 1.5 line spacing. Use 25 mm for all margins. The text length should not exceed 12 A4 pages, including text, tables, images, graphs/charts, references, and other attachments.

The title page should contain the title of the paper in English, followed by the title in Serbian, with font size 14 pt, Bold. After a space, please provide the author's full name, title, affiliation (workplace **with the mandatory inclusion of the country)**, email address, and contact phone number, using font size 12 pt. If the author has an ORCID number, it should be included immediately after the author's name. For more information about ORCID iD, please visit: https://orcid.org and after registration, enter your ORCID iD number in the paper.

Next, leave a space and write an abstract, up to 250 words, in English, followed by the abstract in Serbian, both in size 12 pt. The abstract should provide a brief informative summary of the article, enabling readers to quickly and accurately assess its relevance. Authors should explain the

research objective or the reason for writing the article. Then, they need to describe the methods used in the research and briefly summarize the obtained results.

Keywords should be listed after one line of spacing below the abstract, in English, followed by the keywords in Serbian. There should be a maximum of five keywords, size 12 pt, Italic. Then leave a space of two lines before the main text of the paper begins.

Texts should be concise, written in a clear style, and follow a logical sequence that typically includes: an introduction, main body of the paper, and conclusion. The font size for the main text is 12 pt. Headings and subheadings in the text should be 12 pt, Bold.

The title and number of illustrations (diagrams, photographs, graphs/charts) should be centered above the illustration, size 12 pt. The title and number of tables should also be centered above the table, size 12 pt. The source must be stated ("Source: …") below the illustration or table, size 10 pt. If the results presented graphically or in tables are from the author's research, the source below the illustration or table should be: Author's research.

If the author wishes to include acknowledgments or references to project(s) under which the text was written, they should do so in a separate section titled "Acknowledgments", following the Conclusion in sequence and preceding the author's affiliation and the abstract in Serbian.

For writing references, use the APA (Publication Manual of the American Psychological Association) international standard for writing references. Notes or footnotes may contain additional explanations or comments related to the text. Footnotes should be written in Times New Roman font, size 10 pt.

In APA style, the source being cited is mentioned **within the text**, with the elements (author, year of publication, page number of the quoted section) enclosed in parentheses immediately before the period and separated by commas.

RULES FOR IN-TEXT CITATIONS

When citing a source written by a single author:

If the author's name appears in the sentence, the year of publication of the cited text is placed in parentheses immediately after the author's name, and the page number is provided at the end of the sentence:

Example:

As Besermenji (2007) highlights, “air pollution is a particularly prevalent issue, primarily due to an exceptionally low level of environmental awareness and a lack of professional education in the field of environmental protection” (p. 496).

If the author’s name does not appear in the sentence, the author’s last name, year of publication, and page number are placed in parentheses at the end of the sentence:

Example:

Also, “rural tourism is expected to act as one of the tools for sustainable rural development” (Ivolga, 2014, p. 331).

Note: If the citation is a paraphrase or summary, the page number is not necessary.

Example:

The environment encompasses everything that surrounds us, or everything that is directly or indirectly connected to human life and production activities (Hamidović, 2012).

When citing a source written by two authors:

Use “and” or “&” between the authors’ last names, depending on whether the authors are mentioned in the sentence.

Examples:

Chaudhry and Gupta (2010) state that as many as 75% of the world’s poor live in the rural areas, and more than one-third of rural areas are in arid and semiarid regions.

Hence, “rural development is considered as a complex mesh of networks in which resources are mobilized and in which the control of the process consists of interplay between local and external forces” (Papić & Bogdanov, 2015, p. 1080).

When citing a source written by 3-5 authors:

For the first-time citation, list all authors:

Example:

(Cvijanović, Matijašević Obradović, & Škorić, 2017)

For subsequent citations, list only the first author followed by “et al.”:

Example:
(Cvijanović et al., 2017)

When citing a source written by 6 or more authors:

For both the first and subsequent citations, list only the first author followed by "et al.":

Example:
(Savić et al., 2010)

When citing a text authored by an organization:

If the author of a paper is an organization, include the organization's name in parentheses as the author. If the organization has a known abbreviation, provide the abbreviation in square brackets after the full name in the first citation, and use only the abbreviation in all subsequent citations.

Example:
First citation: (Serbian Academy of Sciences and Arts [SASA], 2014)
Subsequent citations: (SASA, 2014)

When citing texts by authors with the same surname:

Use the authors' initials to avoid confusion.

Example:
The viewpoint expressed by D. Savić (2017) has been presented...

When citing multiple references by the same author from the same year:

If there are two or more references from the same author in the same year, add letter designations "a", "b", etc., after the year.

Example:
(Dragojlović, 2018a)
(Dragojlović, 2018b)

When citing two or more texts in one citation:

List the authors' last names in the order of publication and separate them with a semicolon.

Example:
Obviously, living and working in rural areas has always been connected with specific material and symbolic relations to nature (Milbourne, 2003; Castree & Braun, 2006).

When citing a newspaper article with a specified author:

Example:

It was reported in *NS uživo* (Dragojlović, 2021) that...

In the reference list, format this reference as follows:

Dragojlović, J. (2021). Anketirani Novosađani za vraćanje smrtne kazne u Ustav [Novi Sad residents surveyed to return the death penalty to the Constitution]. *NS uživo*, January 22.

When citing a newspaper article without a specified author:

Example:

As published in *Politika* (2012)

In the reference list, format this reference as follows:

Politika. (2012). Straževica gotova za dva meseca [Straževica finished in two months]. February 1.

When citing personal correspondence:

Example:

According to Nikolić (2020),

In the reference list, format this reference as follows:

Nikolić, A. (2020). Pismo autoru [Letter to the author], November 21

When citing a text in press:

At the end of the reference, before the period, add "in press."

When citing court decisions, the practice of the European Court of Human Rights, and other sources from domestic and international judicial practice:

The reference should contain as complete information as possible: type and number of the decision, date when the decision was brought, publication in which it was published.

Example in text:

(Decision of the High Court in Belgrade – Special Department K.Po1 no. 276/10 dated January 26, 2012)

Example in text: (Borodin v Russia, par. 166.)

Note:

Sources from judicial practice **should not be listed** in the reference list. The full reference **should be provided** in a footnote. When citing the practice of the European Court of Human Rights, the application number should also be included.

Example for reference in a footnote:

As stated in the Decision of the High Court in Belgrade – Special Department K.Po1 no. 276/10 from January 26, 2012. Intermex (2012). Bilten Višeg suda u Beogradu [Bulletin of the High Court in Belgrade], 87, p. 47.

Borodin v Russia, application no. 41867/04, ECHR judgment, February 6, 2013, par. 166.

When citing laws and other regulations:

When citing a legal text or other regulation, mention the full name of the law or regulation and the year it came into force.

Example:

(Criminal Procedure Code, 2011)

(Regulation on the Content of the Decision on the Implementation of Public Procurement Procedure by Multiple Clients, 2015)

This rule also applies to laws or other regulations that are no longer in force.

Example:

(Criminal Code of the Republic of Serbia, 1977)

When citing international regulations, it is sufficient to mention the abbreviated name of the document along with its number and the year it was adopted.

Example:

(Regulation No. 1052/2013) or (Directive 2013/32)

When citing a text with an unknown publication date or author:

For works with an unknown date, use "n.d." (non-dated) in place of the year.

Example:

Their significance for parliamentary processes is immeasurable (Ostrogorski, n.d.).

If the paper uses a reference to a paper by an unknown author, cite the title of the paper and include the year if known.

Example:

All that has been confirmed by a mixed, objective-subjective theory (Elements of a criminal offense, 1986, p. 13).

Important Note:

Cited sources (regardless of the language in which they are written) should not be translated into English, except for the titles of papers (publications, legal acts) which should be translated and written in square brackets.

Example:

1. Matijašević Obradović, J. (2017). Značaj zaštite životne sredine za razvoj ekoturizma u Srbiji [The importance of environmental protection for the development of ecotourism in Serbia]. *Agroekonomika*, *46*(75), pp. 21-30.
2. Jovašević, D. (2017). *Krivična dela ubistva* [*Murder as a Crime*]. Beograd: Institut za kriminološka i sociološka istraživanja.
3. Uredba o ekološkoj mreži Vlade Republike Srbije [The Ecological Network Decree of the Government of the Republic of Serbia]. *Službeni glasnik RS*, br. 102/10.
4. Zakon o turizmu [The Law on Tourism]. *Službeni glasnik RS*, br. 17/19.

References Section:

At the end of each manuscript, include a **"References"** section listing all the cited sources in alphabetical order. Titles in foreign languages that begin with definite or indefinite articles ("a", "the", "Die", etc.) should be listed as if the article does not exist. The list of references should include only works that are published or accepted for publication.

The editorial board emphasizes the usage of recent references whenever possible, which will be a key criterion when selecting manuscripts for publication. Each reference must include a DOI number if available. If the cited reference does not have a DOI number, the author may include a URL.

Example of referencing with a DOI number:

Počuča, M., & Matijašević Obradović, J. (2018). The Importance of Evidence Collection in Procedures for Criminal Acts in the Field of Economic Crime in Serbia. In: Meško, G., et al. (eds.), *Criminal Justice and Security in Central and Eastern Europe: From Common Sense to Evidence-based Policy-making* (pp. 671-681). Maribor: Faculty of Criminal Justice and Security and University of Maribor Press. DOI: 10.18690/978-961-286174-2

Example of referencing with a URL:

Milosavljević, B. (2015). Pravni okvir i praksa primene posebnih postupaka i mera za tajno prikupljanje podataka u Republici Srbiji [Legal framework and practice of application of special procedures and measures for secret data collection in the Republic of Serbia]. In: Petrović, P. (Ed.), *Posebne mere tajnog prikupljanja podataka: između zakona i sudske prakse* [*Special measures for secret data collection: between law and case law*] (pp. 5-33). Beograd: Beogradski centar za bezbednosnu politiku. Downloaded 2021, January 15, from https://bezbednost.org/wp-content/uploads/2020/06/posebne_mere_tajnog_prikupljanja_podataka__vodic_.pdf.

Examples of references to be listed at the end of the manuscript:

References

1. Agencija za privredne registre. Privredna društva [Companies]. Downloaded 2020, January 10 from https://www.apr.gov.rs/o-agenciji.1902.html
2. California Secretary of State. Downloaded 2020, December 15 from https://www.sos.ca.gov/business-programs/
3. Dukić-Mijatović, M. (2011). Korporativno upravljanje i kompanijsko pravo Republike Srbije [Corporate Governance and Companies Business Law of the Republic of Serbia]. *Pravo – teorija i praksa*, *28* (1-3), pp. 15-22.

4. Dragojlović, J., & Bingulac, N. (2019). *Penologija između teorije i prakse* [*Penology between theory and practice*]. Novi Sad: Pravni fakultet za privredu i pravosuđe u Novom Sadu.
5. Dragojlović, J. (2021). Anketirani Novosađani za vraćanje smrtne kazne u Ustav [Novi Sad residents surveyed to return the death penalty to the Constitution]. NS uživo, January 22.
6. Gopalsamy, N. (2016). *A Guide to Corporate Governance.* New Delhi: New Age International.
7. Jesover, F., & Kirkpatrick, G. (2005). The Revised OECD Principles of Corporate Governance and their Relevance to Non-OECD Countries. *Corporate Governance: An International Review*, *13* (2), pp. 127-136. DOI: 10.1111/j.14678683.2005.00412.x
8. Milosavljević, B. (2015). Pravni okvir i praksa primene posebnih postupaka i mera za tajno prikupljanje podataka u Republici Srbiji [Legal framework and practice of application of special procedures and measures for secret data collection in the Republic of Serbia]. In: Petrović, P. (ured.), *Posebne mere tajnog prikupljanja podataka: između zakona i sudske prakse* [*Special measures for secret data collection: between law and case law*] (pp. 5-33). Beograd: Beogradski centar za bezbednosnu politiku. Downloaded 2021, January 15 from https://bezbednost.org/wpcontent/uploads/2020/06/posebne_mere_tajnog_prikupljanja_podataka_-_vodic_.pdf
9. Počuča M., & Matijašević Obradović, J. (2018). The Importance of Evidence Collection in Procedures for Criminal Acts in the Field of Economic Crime in Serbia. In: Meško, G., et al. (eds.), *Criminal Justice and Security in Central and Eastern Europe: From Common Sense to Evidence-based Policy-making* (pp. 671-681). Maribor: Faculty of Criminal Justice and Security and University of Maribor Press. DOI: 10.18690/978-961-286-174-2
10. Regulation (EU) No. 1052/2013 establishing the European Border Surveillance System (Eurosur), OJ L 295 of 6/11/2013.
11. Škorić, S. (2016). *Uticaj poslovnog imena privrednog društva na njegovo poslovanje – doktorska disertacija* [*The influence of the business name of the company on its business – doctoral thesis*]. Novi Sad: Pravni fakultet za privredu i pravosuđe u Novom Sadu.
12. Škulić, M. (2007). *Krivično procesno pravo* [*Criminal Procedural Law*]. Beograd: Pravni fakultet Univerziteta u Beogradu i JP Službeni glasnik.

13. Uredba o ekološkoj mreži Vlade Republike Srbije [The Ecological Network Decree of the Government of the Republic of Serbia]. *Službeni glasnik RS*, br. 102/10.
14. Veljković, N. (2017). *Indikatori održivog razvoja: Srbija i svet* [*Sustainable development indicators: Serbia and the world*]. Downloaded 2017, October 22 from http://indicator.sepa.gov.rs/o-indikatori
15. Zakonik o krivičnom postupku [Criminal Procedure Code]. *Službeni glasnik RS*, br. 72/11, 101/11, 121/12, 32/2013, 45/13, 55/14 i 35/19.

Pravni fakultet za privredu i pravosuđe u Novom Sadu
Univerziteta Privredna akademija

PRAVO teorija i praksa
2 / 2025

Pravni fakultet za privredu i pravosuđe u Novom Sadu
Univerzitet Privredna akademija

Novi Sad, Geri Karolja 1
Tel: 021/400-499,
469-513, 469-518
www.pravni-fakultet.edu.rs