Glasnik za društvene nauke, **Vol. XVIII, God. XVIII (Broj 1)**
***Journal of Social Sciences*, Vol. XVIII, Year XVIII (Issue 1)**

DOI: 10.46793/GlasnikDN18.1.237M Research paper
UDK 343.53:004.7
[004:007]:004.056

Sofija Milenković[*]
Faculty of Security Studies, University of Belgrade, Belgrade, Serbia
Sanela Veljković[†]
Vinča Institute of Nuclear Sciences – National Institute of the Republic of Serbia, Belgrade, Serbia
Anita Klikovac[‡]
Faculty of Security Studies, University of Belgrade, Belgrade, Serbia

Received: March 07, 2026
Returned for revision: March 23, 2026
Accepted: June 4, 2026

CRIMINAL LAW PROTECTION OF INFORMATION SECURITY IN THE CONTEXT OF COMPUTER FRAUD

Abstract
Globalization, development of new and increasingly advanced information and communication technologies and relocation of communications and activities from physical to cyber space have created an abundance of opportunities as well as risks. Protecting cyber space in the virtual world has become just as crucial as protecting the national borders in the real one. The expansion of new entities – social networks – at the beginning of

[*] E-mail address: sofijamilenkovic.fb@gmail.com, ORCID ID: https://orcid.org/0009-0002-3426-0487
[†] E-mail address: sanela.veljkovic@vin.bg.ac.rs, ORCID ID: https://orcid.org/ 0009-0003-3650-290X
[‡] E-mail address: anitaklikovac@yahoo.com, ORCID ID: https://orcid.org/0009-0003-8616-7564

21st century, has opened up new domains for high-tech crime and various abuses of computer data that are generally driven by economic interest. The most common type of high-tech crime is computer fraud, abusing data and thus affecting their electronic processing and transmission, in turn causing extremely harmful consequences for the citizens, state and society. It is concluded that it is up to the state authorities and legislators to gain on technological development to be able to timely prevent such criminal acts using appropriate legal regulations, preventive, educational and other coordinated measures, i.e. to adequately sanction them, in order to provide the required levels of security to both individual users and society as a whole.

Key words: *information security, high-tech crime, cyberspace, computer fraud.*

JEL classification: H56, K42, L86, O33

Introduction

The rapid advancement of digitalization, accompanied by the proliferation of technological innovations and novel communication tools, has profoundly influenced contemporary social and political processes. The pursuit of dominance in cyberspace and information superiority has become particularly prominent in interstate relations in the twenty-first century [1]. At the same time, the digital environment has created opportunities for entirely new forms of illicit conduct, specific to the electronic age [2]. By facilitating innovative methods of propaganda dissemination and disinformation campaigns, information and communication technologies (ICTs) have indirectly affected existing social relations and the exercise of a broad spectrum of fundamental human rights and values [3], frequently raising questions regarding the adequacy of their protection under criminal law.

Modern technology serves not only as the foundation for the functioning and protection of cyberspace but also as a platform for conducting attacks against information systems, including the disruption of government websites, the insertion of false data into an adversary's information systems, and other forms of malicious cyber

activity [3]. The concept of "cyberspace" emerged and developed in the United States alongside advances in computer science and information and communication technologies. The Internet as a global network, within the framework that is now commonly referred to as cyberspace, was technologically developed between the late 1960s and the early 1990s for industrial, scientific, and defense-related purposes through a series of projects, most notably the ARPANET initiative of the United States Department of Defense [4, pp. 51–53].

The subsequent evolution of cyberspace has occurred in parallel with broader technological and societal developments, which explains the absence of a universally accepted definition of the concept. Nevertheless, as Mladenović observes [4, p. 70], there is broad scholarly consensus that cyberspace constitutes a virtual environment created through the application of information and communication technologies and computer science, enabling the processing, storage, exchange, and management of data and information. Consequently, the effective organization and management of information systems are essential for establishing a robust framework capable of mitigating both human and systemic errors and minimizing potential security risks [5, p. 133].

Cyberspace may be understood as any virtual environment forming part of the broader information ecosystem, which encompasses computers, computer networks, and information systems. Within this environment, computers, information systems, and networks may serve either as instruments for compromising information, national, or personal security, or as targets and means of perpetrating criminal offenses. In this regard, Aleksić and Škulić [6, p. 382] emphasize that this form of criminal activity manifests through the use, damage, misuse, or other forms of manipulation of the two fundamental components of computer systems: hardware and software.

Given the distinctive characteristics of cyberspace and the technologies operating within it, criminal law scholarship commonly employs the terms "cybercrime," "computer crime," and "computer-related crime" to describe this category of offending. Unlike Serbian

legislation, which does not differentiate between these concepts, the Anglo-American legal and academic tradition generally uses the term "computer crime" to refer to offenses involving computer systems in the physical world, whereas "cybercrime" denotes offenses that necessarily involve the use of computer networks or cyberspace as an operational environment. Although the conceptual boundaries between these terms remain indistinct, it may be argued that the term "high-tech crime" provides the most comprehensive designation for encompassing both forms of criminal activity within the legal framework of the Republic of Serbia [7]. Furthermore, due to their inherently transboundary nature and the challenges they pose to traditional notions of territorial jurisdiction, such offenses are increasingly regarded as falling within the broader category of transnational crime.

1. Research Subject, Problem, Objectives, and Methodology

The subject of this paper is the analysis of information security in the context of criminal law protection against computer fraud in the Republic of Serbia.

The research problem arises from the discrepancy between the rapid development of information and communication technologies and the capacity of legal systems to effectively respond to emerging forms of abuse involving computer data and information systems. As technological advancements continue to expand the scope and sophistication of cyber-enabled criminal activities, legal frameworks are increasingly challenged to provide adequate protection and effective enforcement mechanisms.

The primary objective of this study is to examine the security and criminal law dimensions of computer fraud, analyze the normative framework governing this area in the Republic of Serbia, and identify the principal challenges associated with the protection of data and information in contemporary cyberspace.

The purpose of the research is to identify the legal and institutional limitations of the existing protection system and to formulate recommendations aimed at enhancing information security and strengthening the prevention of computer fraud. Particular

attention is devoted to assessing the effectiveness of the current regulatory framework and its capacity to address the evolving nature of cyber threats.

The study employs a qualitative research methodology based on the analysis of relevant domestic and international scholarly literature, applicable legislation of the Republic of Serbia, international legal instruments, and available statistical data pertaining to information security and high-tech crime.

The research is grounded in the application of the normative-legal method, content analysis, and the comparative method. The normative-legal method is utilized to examine the criminal law and regulatory framework governing the protection of computer data and the prosecution of computer fraud. Content analysis is applied to the examination of legal sources, academic literature, and institutional reports, while the comparative method is employed to compare selected solutions within Serbian legislation with relevant European legal instruments and international standards in the field of cybersecurity and cybercrime.

2. Information Security in Cyberspace

Information security may be defined as a set of measures designed to ensure that data processed through information and communication technology systems are protected against unauthorized access, while preserving their integrity, availability, authenticity, and non-repudiation, thereby enabling the uninterrupted functioning of the system. In this regard, ICT security measures comprise both technical and organizational mechanisms intended to manage and mitigate security risks affecting ICT systems (Article 2 of the Law on Information Security of the Republic of Serbia). Given that data and information have become strategic resources of the twenty-first century [3, pp. 87–88], ensuring the adequate protection of information systems is a matter of significant national interest. As Aleksić and Škulić [6] observe, a particularly concerning issue is the reluctance of many companies to report incidents involving computer fraud and other forms of cyber abuse. Such organizations often fear that disclosure would reveal deficiencies in their security capabilities

and adversely affect their market position and reputation. At the same time, private companies themselves are frequently involved in the misuse or inadequate handling of employees' and users' personal data.

According to data published by the Statistical Office of the Republic of Serbia in 2025, more than 90% of internet users in Serbia access the Internet on a daily or near-daily basis, compared with 85.4% in 2023, while 84.7% of internet users maintain social media accounts, compared with 82.3% in 2023 [26]. For comparison, according to the Digital Economy and Society Index (DESI) [11, 12], 87% of individuals aged 16 to 74 within the European Union regularly used the Internet in 2021, with the highest rates recorded in the Netherlands and Finland. By 2023, this proportion had increased to 91%. However, only approximately 54% of respondents in 2021 and 56% in 2023 possessed at least basic digital skills, raising important concerns regarding their ability to maintain personal security in cyberspace. Notably, 83% of respondents reported never having informed the relevant authorities that they had been victims of cybercrime, for a variety of reasons.

A particularly significant development has been the rapid increase in the use of artificial intelligence tools. In 2024, the adoption of AI technologies accelerated considerably, while approximately 32.7% of EU citizens reported using generative artificial intelligence applications, such as ChatGPT, in 2025. Given persistent concerns regarding digital literacy, particularly the ability to critically assess information and understand cybersecurity risks associated with the use of such technologies, the European Union has established the strategic objective of ensuring that 80% of its citizens acquire at least basic digital competencies by 2030 [27].

According to data published by the National Computer Emergency Response Team (CERT) of the Republic of Serbia, the number of reported incidents affecting critical information and communication systems demonstrates a continuing upward trend in various forms of cyber abuse. Reports for 2023 and 2024 indicate that fraud-related incidents, including phishing attacks, unauthorized use of resources, and other forms of data and information system

misuse, remain among the most frequently reported categories. Particularly noteworthy is the finding of the Regulatory Authority for Electronic Communications and Postal Services (RATEL) that fraud-related incidents constituted the largest category of reported cybersecurity incidents in 2024, underscoring the significant presence of this form of high-tech crime within the domestic cyber environment.

As Stojanović argues [9, p. 663], due to the specific nature of the subject matter, criminal law protection aimed at safeguarding the lawful use of information technologies constitutes a subsidiary, additional form of protection. Other issues relating to security, technological efficiency, and the capabilities of emerging technologies largely remain within the domain of technological prevention and risk management. Consequently, criminal law protection in cyberspace typically becomes relevant only after a cyberattack has occurred and harmful consequences have already materialized.

3. Security of Computer Data and Computer Fraud

In order to prevent the misuse of electronically processed data, the Criminal Code of the Republic of Serbia (hereinafter: CC) places particular emphasis on preventing technically sophisticated attacks aimed at obtaining unauthorized access to protected ICT systems. Such attacks typically involve prolonged, multi-stage operations requiring substantial planning and preparation (Chapter XXVII of the Criminal Code – Criminal Offences Against the Security of Computer Data). In addition, the scope of high-tech crime is further defined by the Law on the Organization and Jurisdiction of Government Authorities in Combating High-Tech Crime. This legislation regulates, inter alia, the establishment, organization, jurisdiction, and powers of specialized units within the Public Prosecutor's Office and the Ministry of the Interior responsible for the detection, prosecution, and adjudication of high-tech crime offenses.

Statistical data from the Public Prosecutor's Office indicate a continuous increase in reported cases of high-tech crime in the

Republic of Serbia, with unauthorized access to computer networks and various forms of fraud accounting for the largest share of reported offenses [14]. The criminal offence of computer fraud encompasses a broad spectrum of unlawful online activities primarily aimed at obtaining unlawful financial gain. As Aleksić and Škulić [6, p. 381] observe, defining computer crime requires a comprehensive approach based on three fundamental elements: the method of commission, the means employed, and the consequences of the criminal conduct. Among the most common forms of online criminal activity are fraud schemes associated with online auction platforms and e-commerce websites, payment card fraud, so-called "Nigerian scams," and Distributed Denial-of-Service (DDoS) attacks [15, p. 90]. A particularly concerning issue is the relatively limited body of judicial practice compared to the number of reported cases and imposed sanctions for computer fraud. This disparity raises important questions regarding the practical effectiveness of legal protection afforded to data and information, as well as the challenges associated with proving and prosecuting this offense.

According to Prlja, Ivanović, and Reljanović [16, p. 46], the intention of the Serbian legislator was to protect the authenticity and integrity of data processed or transmitted electronically. In many cases, computer fraud is committed by highly organized cybercriminal groups operating across national borders and specializing in particular regions or methods of data acquisition.
Similarly, Lazarević [17, p. 884] emphasizes that the primary legal interest protected by the offense of computer fraud is the authenticity and integrity of electronically processed and transmitted computer data.

Given the frequently transnational nature of these offenses and the borderless character of cyberspace, determining the applicable law often presents significant practical challenges. Such difficulties arise, inter alia, from the fact that criminal offenses contained in international conventions become enforceable only after their incorporation into domestic criminal legislation and the entry into force of the relevant national legal provisions [18, pp. 26–31]. Nevertheless, one of the defining characteristics of computer fraud

remains the difficulty of obtaining and presenting sufficient evidence, despite the considerable public attention that such cases often attract [19, p. 205].

A notable example is the so-called "419 Scam," commonly referred to as the "Nigerian Scam," which emerged in the early 1980s and has caused financial losses amounting to millions of dollars worldwide. These schemes are typically associated with organized criminal groups specializing in Internet-based fraud [16, pp. 54–55]. Furthermore, perpetrators of cyber-enabled offenses are not limited to individual actors such as hackers, terrorists, or other malicious users. State actors, private corporations, hacktivist groups, and other organizations may also engage in activities that threaten information security, particularly given the widespread commercial availability of technologies capable of being integrated into cyber operations [3, p. 89].

As Stojanović and Perić [20, p. 256] argue, the offender is typically a person possessing the practical capability to compromise information systems or networks through activities such as hacking, the deployment of computer viruses, worms, Trojan horses, or similar malicious software. Conversely, virtually any individual who fails to exercise adequate caution in cyberspace may become a victim of fraud. In practice, victims themselves frequently provide the most valuable source of information for investigations, having fallen victim through interactions with fraudulent websites, deceptive online advertisements, or unsolicited commercial communications (spam).

Among the most common mistakes made by computer users is the belief that they have "nothing to hide" and are therefore unlikely to become targets of cybercrime, as well as excessive trust in companies to which they voluntarily disclose personal information, often resulting in the failure to implement additional protective measures [21, p. 683].

At the same time, competent authorities report a continuous increase in criminal complaints related to high-tech crime. A substantial proportion of these cases involve unauthorized access to information systems, online fraud schemes, and the misuse of digital

data. Reports issued by prosecutorial authorities and specialized high-tech crime units indicate that the expansion of digital services and the growing number of Internet users have been accompanied by a corresponding increase in reported cyber-enabled offenses. In addition to traditional forms of unauthorized access to computer systems, authorities are increasingly confronted with phishing campaigns, payment card fraud, and various forms of social engineering, all of which place additional demands on institutions responsible for the detection, investigation, and prosecution of cybercrime.

Criminal acts constituting computer fraud are frequently preceded by specific deceptive practices that function as techniques for manipulating users of information and communication systems, such as social engineering, phishing, and related methods, with the ultimate objective of gaining unauthorized access to a targeted system. Unlike these forms of cyberattacks, the offense of computer fraud requires that one of the prescribed acts of commission influence the outcome of electronic data processing or data transmission [6, p. 385]. Consequently, unlike preparatory deceptive practices such as phishing or social engineering, the defining consequence of computer fraud is an alteration of the result of electronic data processing that would not have occurred in the absence of the offender's conduct. For example, sports betting platforms are frequently targeted by computer fraud schemes in which the perpetrator gains unauthorized access to the system and modifies a single parameter, such as the system time setting. Such manipulation may enable the offender to obtain unlawful financial gain while simultaneously causing financial damage to the betting operator [15, p. 102].

With regard to criminal sanctions, the question is whether greater emphasis should be placed on preventive mechanisms, in light of the relatively lenient sentencing practices observed in many cases, as well as the considerable period of time that frequently elapses between the commission of the offense and the enforcement of the final judgment.

In this context, Stojanović [20] emphasizes that criminal law protection is not achieved solely through the threat or imposition of punishment but also through a broader and more complex system of social control. Consistent with this perspective, Kolarević [25] highlights the importance of continuous improvement as an essential component of a comprehensive strategy for combating cybercrime and enhancing information security.

4. Criminal Law and Institutional Framework for Protection

The protection of information security in the Republic of Serbia is based on a combination of normative and institutional mechanisms aimed at preventing abuses in cyberspace, identifying offenders, and ensuring criminal law protection of data and information systems. The rapid development of information and communication Particular importance in this regard is attributed to the Law on Information Security, the Criminal Code of the Republic of Serbia, and the Law on the Organization and Jurisdiction of Government Authorities in Combating High-Tech Crime. This institutional framework facilitates the concentration of expertise and the development of specialized capacities required for handling complex cases that frequently possess an international dimension.

The Law on Information Security constitutes the primary legal instrument governing the protection of information and communication technology systems against security risks and incidents. It establishes security requirements, defines the obligations of operators of critical ICT systems, and regulates the competencies of the National Computer Emergency Response Team (CERT) in the areas of prevention, coordination, and response to cybersecurity incidents. The significance of this legislation lies in its recognition that information security cannot be achieved solely through the punishment of offenders after the commission of a criminal offense, but also through the development of resilient systems and the timely identification of security threats [28, 29].

From an institutional perspective, specialized organizational units within the Ministry of the Interior perform a central role in the detection, investigation, and documentation of cybercrime offenses.

Given that computer fraud and other forms of cybercrime are often linked to transnational criminal networks, cooperation with international law enforcement and security organizations constitutes a particularly important aspect of their activities. In this regard, on June 1, 2026, the digital platform of the Ministry of the Interior for reporting internet fraud and high-tech crime "Cyber Straža" was officially launched, which was conceived as a centralized portal for reporting crimes and information from the field of high-tech crime that will provide citizens with direct protection from internet fraud [13].

At the prosecutorial level, the Special Department for High-Tech Crime within the Higher Public Prosecutor's Office in Belgrade occupies a central position in the criminal prosecution of cybercrime offenders. The importance of this institution derives from the fact that cybercrime investigations require specialized technical expertise, rapid information exchange, and continuous monitoring of emerging forms of abuse within the digital environment.

The foregoing demonstrates that effective criminal law protection of information security depends not only on the existence of appropriate legal norms but also on the efficiency and capacity of the institutions responsible for their implementation.

The development of information and communication technologies and society's increasing dependence on digital systems has also created the need for a coherent European framework for information security protection. Unlike traditional approaches, which primarily focused on sanctioning offenders after the commission of criminal offenses, the contemporary European approach is based on a combination of preventive, organizational, technical, and criminal law mechanisms. Among the most significant instruments in this field are the NIS2 Directive, the General Data Protection Regulation (GDPR), the Council of Europe Convention on Cybercrime (Budapest Convention), and the European Union Cybersecurity Strategy.

These instruments collectively reflect a shift from reactive approaches toward a more comprehensive model of cybersecurity governance based on risk management, resilience building,

international cooperation, and the protection of fundamental rights in the digital environment. At the same time, they establish minimum standards for the protection of information systems and personal data, strengthen incident reporting obligations, and encourage closer cooperation among public authorities, private-sector entities, and international partners in addressing increasingly sophisticated cyber threats:

4.1. NIS2 Directive

Directive (EU) 2022/2555, known as the NIS2 Directive, constitutes a fundamental European Union instrument for strengthening the cybersecurity of critical infrastructure and entities providing essential and important services. Compared to its predecessor, the original NIS Directive, NIS2 significantly expands the scope of entities to which it applies and introduces more stringent obligations regarding risk management, incident reporting, and the accountability of organizational leadership. A key feature of this Directive is its preventive approach to information systems security. While criminal law protection is typically activated after the commission of a criminal offense, NIS2 seeks to prevent security incidents by establishing comprehensive security standards and structured risk management frameworks. In this sense, the Directive complements criminal law protection and reflects a broader shift toward understanding cybersecurity as a continuous governance process rather than solely a matter of post hoc sanctioning.

4.2. General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) represents the most significant European Union legal instrument in the field of personal data protection. Its primary objective is to ensure individuals' control over their personal data and to prevent its unlawful processing, misuse, or unauthorized disclosure. The relevance of the GDPR to the issue of computer fraud lies in the fact that personal data frequently constitute the primary target of various forms of cybercrime. Phishing attacks, identity theft, and online fraud schemes commonly involve the unlawful acquisition and exploitation

of individuals' personal data. In contrast to the criminal law approach, which is primarily offender-centered and focused on sanctions, the GDPR adopts a rights-based approach, emphasizing the protection of data subjects and the obligations of data controllers and processors. In this way, it provides an additional layer of protection with a strong preventive function.

4.3. Budapest Convention on Cybercrime

The Council of Europe Convention on Cybercrime (2001), commonly referred to as the Budapest Convention, is the first and most significant international legal instrument dedicated to combating cybercrime. Its main objective is to harmonize national criminal legislation, improve investigative capacities, and strengthen international cooperation in the detection, investigation, and prosecution of offenders. For the Republic of Serbia, this Convention holds particular importance, as it has served as a key foundation for the development of national legislation in the field of high-tech crime. It establishes a set of criminal offenses including illegal access to computer systems, illegal interception of data, data interference, system interference, misuse of devices, and computer fraud. Given the transnational nature of most computer fraud cases, the mechanisms of international cooperation provided under the Convention represent one of the most important tools for the effective investigation and prosecution of offenders.

4.4. European Union Cybersecurity Strategy

The European Union Cybersecurity Strategy is a strategic policy document defining the long-term objectives and priorities of the EU in the field of digital security. Unlike the previously discussed instruments, which are primarily of a normative nature, the Strategy performs a developmental and policy-oriented function. It places particular emphasis on strengthening the resilience of critical infrastructure, developing institutional capacities, enhancing cooperation among Member States, and improving capabilities for responding to cyber threats. The Strategy recognizes that contemporary threats are no longer limited to individual computer

systems but may affect the functioning of state institutions, the economy, and society as a whole. In this context, the fight against computer fraud is understood as part of a broader framework for safeguarding cyberspace and maintaining public trust in the digital environment.

5. Comparative Analysis

A comparative analysis demonstrates that the European regulatory framework is not based solely on criminal law repression, but rather on an integrated approach combining prevention, data protection, institutional resilience, and international cooperation. While the Budapest Convention and national criminal law provide the basis for the prosecution of offenders, the GDPR and the NIS2 Directive primarily emphasize harm prevention and the strengthening of information system security.

In this regard, the domestic regulatory framework of the Republic of Serbia is largely aligned with European standards. However, the continued evolution of cyber threats necessitates ongoing improvements in legislation, institutional capacities, and mechanisms of international cooperation in order to ensure an effective and adaptive response to the increasingly complex cyber threat landscape.

Conclusion

The development of information and communication technologies, the digitalization of social processes, and the increasing dependence of individuals, the economy, and state institutions on information systems have led to a significant rise in security risks within cyberspace. Among the most prevalent forms of high-tech crime, computer fraud stands out as a particularly prominent category, enabling the acquisition of unlawful financial gain through the misuse of data, information systems, and users' trust in digital services. An analysis of relevant academic literature, the normative framework, and available institutional reports indicates that computer fraud represents one of the most dynamic and rapidly evolving forms

of criminality, with consequences affecting individuals, economic entities, and the state as a whole.

The conducted analysis demonstrates that the Republic of Serbia has developed a comprehensive normative and institutional framework for information security protection and the suppression of high-tech crime. The Law on Information Security, the Criminal Code of the Republic of Serbia, and the Law on the Organization and Jurisdiction of Government Authorities in Combating High-Tech Crime constitute the foundational pillars of the national protection system. A significant role in its implementation is played by specialized units of the Ministry of the Interior, the Special Department for High-Tech Crime, and the National CERT, whose activities contribute to the detection, prosecution, and prevention of cyber-related abuses.

A comparative analysis of the domestic and European regulatory frameworks indicates that the core solutions of Serbian legislation are largely aligned with international and European standards, particularly the Council of Europe Convention on Cybercrime (Budapest Convention). At the same time, the contemporary European approach increasingly emphasizes prevention, risk management, institutional resilience, and data protection as key elements of digital security governance. While criminal law protection remains an essential instrument for responding to committed offenses, European standards highlight the importance of preventing harm through the development of a cybersecurity culture and the strengthening of organizational and technical protective measures.

A particular challenge arises from the continuously evolving nature of computer fraud, which adapts rapidly to technological development. The increasing prevalence of phishing attacks, digital identity theft, social engineering, and various forms of online fraud confirms that traditional criminal law mechanisms alone are insufficient for the effective suppression of this form of criminality. The transnational character of cyberspace further complicates offender identification, evidence collection, and criminal

prosecution, making international cooperation a key prerequisite for the effective fight against high-tech crime.

Based on the findings of this study, it can be concluded that more effective protection of information security requires the continuous improvement of the normative framework, institutional capacities, and preventive mechanisms. Particular attention should be devoted to strengthening the capacities of specialized state authorities, regularly harmonizing national legislation with European regulatory standards, developing digital literacy and public awareness programs regarding cyber risks, and enhancing cooperation between state institutions, academia, and the private sector. Only an integrated approach that combines legal, technical, organizational, and educational measures can ensure a higher level of information security and more effective protection against computer fraud in the contemporary digital environment.

Acknowledgement
This paper was developed within the framework of the scientific research activities of the Vinča Institute of Nuclear Sciences – National Institute of the Republic of Serbia, funded by the Ministry of Science, Technological Development and Innovation, Grant No. 451-03-33/2026-03/200017.

Bibliography

1. Kilibarda, Z., Mladenović, M. and Ajzenhamer, V. (2014). *Geopolitical Perspectives of the Contemporary World*. University of Belgrade, Faculty of Security Studies, Belgrade.
2. Ashmanov, I. and Kasperskaya, N. (2023). *Digital Hygiene*. Riznica, Belgrade.
3. Putnik, N. (2022). *Cyber War and Cyber Peace*. University of Belgrade, Innovation Center of the Faculty of Security Studies, Akademska misao, Belgrade.
4. Mladenović, D. (2016). *Multidisciplinary Aspects of Cyber Warfare* (PhD dissertation). University of Belgrade, Faculty of Organizational Sciences, Belgrade.

5. Protić, D. (2013). "Information Security: Standards or Rules." *Vojno delo*, 65(1), pp. 133–150.
6. Aleksić, Ž. and Škulić, M. (2011). *Criminalistics*. Faculty of Law, University of Belgrade, Publishing and Information Center, Belgrade.
7. Mandić, J. G., Putnik, N. and Milošević, M. (2017). *Data Protection and Social Engineering – Legal, Organizational and Security Aspects*. Faculty of Security Studies, University of Belgrade, Belgrade.
8. Kovačević, A. and Demić, E. (2023). "Artificial Intelligence for Detecting Fake News on Social Media – Attitudes Analysis." *International Problems*, 75(4), pp. 685–710.
9. Stojanović, Z. (2006). *Commentary on the Criminal Code*. Official Gazette Publishing, Belgrade.
10. Search Engine Journal (2023). "Google Updates Privacy Policy To Collect Public Data For AI Training." Available at: https://www.searchenginejournal.com/google-updates-privacy-policy-to-collect-public-data-for-ai-training/490715/
11. European Commission (2020). *Digital Economy and Society Index (DESI) 2020*. Available at: https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020
12. European Commission (2022). *Digital Economy and Society Index (DESI) 2022*. Available at: https://data.europa.eu
13. RTS (2026). The Ministry of Interior launched the "Cyber watch" platform to protect citizens from internet fraud. Availableat:https://www.rts.rs/lat/vesti/drustvo/5962580/sajber-straza-internet-prevare-sajber-kriminal-mup.html
14. Ministry of Interior of the Republic of Serbia (2024). *High-Tech Crime*. Available at: http://www.mup.gov.rs
15. OSCE Mission in Montenegro (2014). *High-Tech Crime – Practical Guide to Contemporary Criminal Law and Case Examples*. Podgorica. Available at: https://www.osce.org/files/f/documents/5/6/117630.pdf
16. Prlja, D., Ivanović, Z. and Reljanović, M. (2011). *High-Tech Crime Offences*. Institute of Comparative Law, Belgrade.

17. Lazarević, Lj. (2011). *Commentary on the Criminal Code*. Faculty of Law, Union University, Belgrade.
18. Nogo, S. (2016). *International Criminal Law*. Catena Mundi, Belgrade.
19. Dimovski, D. (2010). "Computer Crime." *Proceedings of the Faculty of Law in Niš*, No. 55, pp. 193–210.
20. Stojanović, Z. and Perić, O. (2011). *Criminal Law – Special Part*. Pravni knjiga, Belgrade.
21. Putnik, N., Babić, L. and Kordić, B. (2014). "Socio-psychological and Security Risks of Privacy Violations on Social Networks." In: *Sinteza 2014 – Impact of the Internet on Business in Serbia and Worldwide*, pp. 683–686.
22. Mathew, T. (2004). *Ethical Hacking and Countermeasures*. OSB Publisher, International Council of Electronic Commerce Consultants, New York.
23. Kolarević, D. (2023). *Psychology of Crime*. Criminal Police University, Belgrade.
24. Statistical Office of the Republic of Serbia (2025). *Annual Survey on the Use of Information and Communication Technologies in the Republic of Serbia*. Available at: https://www.stat.gov.rs/sr-latn/vesti/20251024-godisnje-istrazivanje-o-ikt-2025/?a=27&s=0
25. EU4Digital (2021). *2030 Digital Compass: The European Way for the Digital Decade*. Available at: https://eufordigital.eu/library/2030-digital-compass-the-european-way-for-the-digital-decade/
26. Milošević, M. and Putnik, N. (2014). "Problems of Legal (Non-)Regulation of Conflicts in Cyberspace." *Treći program*, 161–162(2), pp. 266–278.
27. National CERT of the Republic of Serbia (2024). *Statistical Report on Security Incidents in ICT Systems of Special Importance*. Available at: https://www.cert.rs/rs/izvestaji.html
28. National CERT of the Republic of Serbia (2023). *Statistical Report on Security Incidents in ICT Systems of Special Importance*. Available at: https://www.cert.rs/rs/izvestaji-arhiva-2024.html
29. National CERT of the Republic of Serbia (2024). "Current Internet Fraud Exploiting the Name of the National Bank of Serbia."

Available at: https://www.cert.rs/rs/obavestenje/1308-Aktuelna-nova-internet-prevara-koja-zloupotrebljava-naziv-Narodne-banke-Srbije.html

30. National CERT of the Republic of Serbia (2024). *Notices Archive 2024*. Available at: https://www.cert.rs/rs/obavestenja-arhiva-2024.html

31. Regulatory Authority for Electronic Communications and Postal Services (RATEL) (2024). *Information Security*. Available at: https://www.ratel.rs/sr/informaciona-bezbednost

Glasnik za društvene nauke, **Vol. XVIII, God. XVIII (Broj 1)**
***Journal of Social Sciences*, Vol. XVIII, Year XVIII (Issue 1)**

КРИВИЧНОПРАВНА ЗАШТИТА ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ У КОНТЕКСТУ РАЧУНАРСКИХ ПРЕВАРА

Сажетак

Глобализација, развој нових и све напреднијих информационо – комуникационих технологија и измештање комуникација и делатности из физичког у сајбер простор отворили су пут бројним могућностима, али и ризицама. Заштита виртуелног, сајбер простора постала је пандан заштити државних граница у реалном свету. Експанзија нових ентитета - друштвених мрежа почетком XXI века отворила је додатни простор за вршење кривичних дела високотехнолошког криминала и за бројне злоупотребе рачунарских података, у позадини којих је најчешће економски интерес. Као најшири вид високотехнолошког криминала издвајају се рачунарске преваре, које путем злоупотребе података утичу на резултат њихове електронске обраде и преноса, чиме узрокују енормне штетне последице по државу, појединце и друштво. На државним органима и законодавцима је да ухвате корак са технолошким развојем и да одговарајућом правном регулативом, превентивним, едукативним и другим координисаним мерама правовремено спрече извршење ових кривичних дела, односно адекватно их санкционишу како би сваком појединцу, али и друштву у целини обезбедили потребан ниво заштите.

Кључне речи: *информациона безбедност, високотехнолошки криминалитет, сајбер простор, безбедност, правни оквир, рачунарска превара.*

JEL klasifikacija: H56, K42, L86, O33