Cybercrime in the Republic of Serbia: Prevalence, Situation and Perspectives

Lazar V. Stošić[1] and Aleksandra V. Janković[2]

[1]Don State Technical University, Rostov-on-Don, Russian Federation
[2]Academy of Professional studies South Serbia – Leskovac,
Department of Preschool Teacher Training School Bujanovac

Article Information*

Review Article • UDC: 343.9.02:004.738.5(497.11)
Volume: 19 Issue: 4, pages: 82–99
Received: July 5, 2022 • Accepted: July 27, 2022
https://doi.org/10.51738/Kpolisa2022.19.4r.82sj

Author Note

Lazar V. Stošić https://orcid.org/0000-0003-0039-7370
Aleksandra V. Janković https://orcid.org/0000-0002-9462-306X

We have no known conflict of interest to disclose.

Corresponding author: Lazar Stošić, Don State Technical University,
Gagarin square 1, Rostov-on-Don, 344000, Russia.
Email: lstoshih@donstu.ru

*Cite (APA):
Stošić, L. V., & Janković, A. V. (2022). Cybercrime in the Republic of Serbia: Prevalence, situation and perspectives. *Kultura polisa*, *19*(4), 82–99. https://doi.org/10.51738/Kpolisa2022.19.4r.82sj

© 2022 by the authors. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

Abstract

The year 2022 was marked by anonymous reports of bombings in schools and other important institutions across Serbia, spread via computers. These events have triggered a public debate on whether the authorities responsible for combating cybercrime can adequately respond to such attacks. As the number of internet users increases, so does the number of potential victims of cybercrime and the obligation of states to protect citizens. Recent events have shown the vulnerability of society to high-tech crime and the risks it poses. The paper analyses the normative and institutional framework for combating cybercrime and data from the Ministry of Internal Affairs on cybercrime. The paper aims to suggest possible changes, based on the analysis of existing cybercrime legislation and the analysis of the institutional framework here and in some European countries, to ensure more effective protection against cybercrime. The paper uses both a normative and a comparative method to present the measures taken in other countries. Descriptive analysis was used to analyze the data collected. The conclusion is that despite a good normative framework, the fight against cybercrime is not adequate, mainly because of the far too small number of staff in special departments and sections of the prosecutor's office and the police compared to the number of crimes, which is increasing year by year. The danger is also that many people are not educated about the dangers of using the internet. Therefore, more attention should be paid shortly to educating citizens of all ages about the dangers and the types of cybercrime.

Keywords: cybercrime, criminal acts, institutions, normative regulation, information technologies

Cybercrime in the Republic of Serbia: Prevalence, Situation and Perspectives

Along with the development of technology, one of the characteristics of modern society is the occurrence of criminal acts precisely through the use of the same technology to commit criminal acts. "The attribute most often attributed to modern society is digital, which is a consequence of the high degree of role and importance of digital technology in daily life... there are no activities of social actors that do not rely more or less on different types of digital technology and modalities of its use" (Stojšić Dabetić, 2021, p. 162). The question is how many users are aware of the dangers of using the internet and the possibility of becoming a victim of a cybercrime. The existence of a culture of security today represents the basic principle of human security, along with the rule of law (Bjelajac, 2021). Cybercrime is the commission of crimes in which the computer is the means or object of the criminal act and in which all potential victims are independent of age, gender and place of residence. The terms: computer crime, electronic crime, e-crime, high-tech crime, cybercrime are also in common use (Sabillon, 2016, p. 166). In the Republic of Serbia, the term high-tech crime is used.

The aim of the work is to propose possible changes, based on the analysis of existing cybercrime legislation and the analysis of the institutional framework, in order to ensure more effective protection against cybercrime. The work uses a normative method to analyse the legal regulations, a comparative method to show the measures taken by countries to protect against cybercrime, and a descriptive analysis to evaluate the data collected.

The most common types of cybercrime are online fraud, cyberbullying, cyber deviance, cyber paedophilia, cyber pornography, the crypto market, etc. (Abu & Israt, 2020, p. 95). The scale of cybercrime is also evident from the data on the involvement of this type of crime relative to other types of crime. For example, we have information that at the global level, cybercrime accounted for 59.5% of the total number of crimes in 2015, and in 2016 this percentage was 82.7%. The data on the targets of the attacks show that the most frequent targets are legal entities at 23%, then state institutions at 21%, individuals at 12% and the rest are various organisations, educational institutions, and the financial sector (Stamenković et. al., 2017, p. 10). According to the Strategy for Combating High-Tech Crime for the Period 2019–2023. (Government, 2018), the Special Department for High-Tech Crime received 2,371 criminal complaints in 2017, which is an increase of more than 15 times compared to ten years earlier when 154 criminal complaints were received in 2007. The largest increase was recorded in 2014 (+68%) and 2015 (+69%). Among other things, the strategy contains data on the structures of criminal offences in the period from 2013 to 2017. Based on this data, the highest percentage of criminal charges, 64%, related to the criminal offence of tax evasion, followed by the criminal offence of harming creditors (22%), criminal offences against intellectual property (9%), criminal offences of display, acquisition and possession of pornographic material and exploitation of a minor for pornography (3%), and criminal offences against the security of computer data (2%) (Government, 2018).

The anonymity that cybercrime affords to perpetrators makes it even more difficult to identify the perpetrator. In some situations, an additional problem in identifying the computer used is identifying the person who used the computer to commit the crime (Sallavaci, 2022, p. 17). Some real-world crimes take place in the virtual world, so predators are increasingly hiding behind computers and anonymity rather than lurking in predator playgrounds. (Bjelajac & Filipović, 2020, str. 260; Stojšić Dabetić, 2021, pp. 164–165). The difficulty in establishing the identity of the perpetrator is one of the reasons for a large number of cybercrimes, precisely because modern technology allows for a high level of anonymity (Me & Pesticcio, 2022). A quick identification process is extremely important in cybercrime files and can be a major problem due to modern technology that complicates the identification process. The identification process means finding and exploring traces that cyber attackers left unintentionally, such as B. the IP address of the origin of the attack. Government agencies need to be careful as attackers often leave false fingerprints to mislead government agencies. In addition, one of the ways of detection is to analyse similar cyberattacks to establish a correlation between them (Pournouri et al., 2022).

The anonymity that cybercrime affords to perpetrators makes it even more difficult to identify the perpetrator. In some situations, an additional problem in identifying the computer used is identifying the person who used

the computer to commit the crime (Sallavaci, 2022, p. 17). Some real-world crimes take place in the virtual world, so predators are increasingly hiding behind computers and anonymity rather than lurking in predator playgrounds. (Bjelajac & Filipović, 2020, str. 260; Stojšić Dabetić, 2021, pp. 164–165). The difficulty in establishing the identity of the perpetrator is one of the reasons for a large number of cybercrimes, precisely because modern technology allows for a high level of anonymity (Me & Pesticcio, 2022). A quick identification process is extremely important in cybercrime files and can be a major problem due to modern technology that complicates the identification process. The identification process means finding and examining traces left unintentionally by cyber attackers, such as: B. the IP address of the origin of the attack. Government agencies need to be careful as attackers often leave false fingerprints to mislead government agencies. In addition, one of the ways of detection is to analyse similar cyberattacks to establish a correlation between them (Pournouri et al., 2022).

Based on the analysis of data from international institutions dealing with cybersecurity and the ranking of countries in the field of cybersecurity (International Telecommunication Union, European Union Agency for Cybersecurity), we found that international institutions do not use the same criteria for measuring the cyber security index in certain countries, which is why the data on the ranking of countries differ. According to research by the International Telecommunication Union (2020), the Global Cybersecurity Index shows countries' commitment to cybersecurity with the aim of helping them identify gaps. One of the studies determined the cybersecurity index of individual countries based on an analysis of five areas: legal measures, technical measures, organisational measures, capacity development measures, and cooperation measures (ITU, 2021, p. vi). Based on the analysis of these five areas, Serbia ranks 33rd out of a total of 182 at the global level, while in Europe it is ranked 25th out of a total of 46 places. The ten best-ranked countries in terms of commitment to cyber security in Europe in 2020 are Great Britain, Estonia, Spain, Lithuania, France, Turkey, Luxembourg, Germany, Portugal, Latvia, and Netherlands (2021, p. 25–27). What these countries have in common and which ranks them in the top ten is the undertaking of measures in the field of education, i.e. the inclusion of materials on cyber security in educational programs in primary, and secondary schools and colleges, training on the subject of cybercrime, a large number of training/campaigns which raise public awareness of the risks of cybercrime, as well as professional training for institutions involved in the prevention, detection and sanctioning of cybercrime, the existence of programs for the certification and accreditation of cyber security professionals (2021). "Building human and institutional capacities is essential to raise awareness, and knowledge in all sectors, for systematic and appropriate solutions, and to promote the development of qualified experts" (2021, p. 133). Another survey published by Enjoy Safer Technology (ESET, 2021) contains data on which cyber countries are the safest. In this research, the ranking criteria used data for the last three years: detected malicious software devices, number of hacked social networks or e-mail accounts, victims of bank card or internet banking fraud, victims of identity theft, and number of cyber security laws. According to this research, the top ten safest cyber countries are Portugal, Lithuania, Slovakia, Greece, Spain, Estonia, Latvia, Finland, Denmark and Slovenia (TBTECH, 2021; ESET, 2021). What these countries have in common is the great importance given to the training of employees in institutions responsible for dealing with cybercrime cases (police, prosecutor's office, judiciary) and the promotion of cybercrime prevention mechanisms. In these countries, "efforts are being made to provide legal actors with more engineering courses and engineers with more legal knowledge" (Ferrara et. al, 2022, p. 64). Another common characteristic of the safest cyber states is the commitment to inform and raise awareness of the public and business sectors, as well as civil society about the dangers of cybercrime (2022). Cyber security in these countries is also due to the number of people working in specialized units, which is in line with the number "considered necessary depending on the scope of the relevant cases" (2022, p. 749).

Criminal Acts of Cybercrime

Criminal acts against the freedoms and rights of people and citizens, which are carried out with the aid of computers, fall under the jurisdiction of state special agencies for combating high-tech crime. These offences include hating speech online based on race, religion, political party, age, disability, sexual orientation, support for a sports club, and other forms of hate that affect social rights, freedom of expression, and liberties (Sabillon et al., 2016, p .172). The cybercrime of identity theft is the theft of someone's identity, the attacker pretends to be someone else in order to gain financial gain (p. 173). Cybercrime Against Sexual Freedom (Viewing, Receiving and Possessing Pornographic Material and Exploiting a Minor for Pornography) (Narodna skupština, 2019). These offences include child pornography, i.e. online pornography involving children (Sabillon et al, 2016, p. 172). Children start using the internet earlier and earlier, so today it is the pre-school age of 4 to 6 years according to some research (Bjelajac & Filipović, 2020). A study (Tomczyk et al., 2022) showed that three-quarters of people (adolescents) use social networks most often just before going to bed and just before waking up. A new generation of children is ready to work with these new technologies, which play an important role in children's learning and acquisition of various cognitive skills (Stošić, 2015), but the question is how informed the children about the potential threats lurking around them. Aside from age, which makes children easy prey, the unlimited amount of time children spend online makes it even easier for criminals to commit crimes against children (Stojšić Dabetić, 2020, p. 164). Disturbed relationships in the family, whether in the form of disagreements between the parents themselves or a bad relationship between the child and the parents, as well as a lack of parental supervision over the child or excessive strictness, are phenomena that lead children to take more time in the family Internet, and that there are greater chances of exposure to cyber pornography and cyber violence (Choi, et al., 2022). Anonymity, i.e., child imitation and naivety, makes it easier for predators to mislead and abuse children (Bjelajac & Filipović, 2020; compare 2021). That virtual world in which young people increasingly find themselves is becoming a place where various security risks hide. The replacement of the real world by a virtual one naturally also brought with it the transfer of certain security risks from one sphere to another (Ilić & Banović, 2021, p. 150). One of the cyber crimes against sexual freedom is revenge pornography, which is committed by disseminating sexual material without consent, and usually, the perpetrator is an ex-partner for revenge or hackers who blackmail victims to gain illegal financial benefits. The consequences of these crimes are extremely difficult for the victims and their lives (Sabillon et al., 2016, p. 174). Last year one such case was a group called "EX-YU Balkan Room" with 36,000 users that posted and shared pictures and videos of naked girls and their phone numbers and addresses. It is a cybercrime, better known as revenge pornography as the images and videos are mostly posted by ex-partners. That only the administrator of the group was arrested while the other 36,000 participants were not even heard is disappointing (Petrović, 2021, p. 4).

Criminal acts against intellectual property do not fall under the exclusive jurisdiction of state agencies responsible for combating high-tech crime, but the act depends on whether a computer or computer system was used as a means or object in the execution, including acts of violation of the moral rights, unauthorised use of the author's work or related rights items, unauthorised removal or alteration of electronic copyright and related rights information, unauthorised use of someone else's design, etc.

Crimes against computer data security include unauthorised access to the computers, the network and data processing. This group of cybercrimes includes cyberespionage (cyber espionage), where the action is the unauthorised recording of others and their conversations and data. “The attackers require the victim to pay a certain amount of money to avoid the damage they threaten to do by stealing or deleting data, deploying ransomware and asking the victim for bitcoin payment” (Sabillon, 2016, p. 173). Ransomware is a type of software used by cyber criminals to lock data and demand a ransom for it. In 50% of cases, in addition to the usual threat of data deletion, it also includes a threat of publication of the data (National Crime Agency, 2021, p. 46).

Cyber-laundering is a term used to denote acts where money obtained through criminal activity is funnelled into legal streams to lose its origin (Sabillon, 2016, p. 173). A large number of cyber crimes consists of cyber fraud (online fraud), i.e., fraud using computer technology such as Internet auctions, credit card fraud, telemarketing fraud, deceptive advertising schemes, "Nigerian" fraud, SMS fraud, manufacturing and introduction of computer viruses, hacking, manufacturing, obtaining and providing funds to others to commit criminal acts against the security of computer data, etc. Computer data corruption (cybervandalism) is the erasure of data and damage to software. Computer sabotage (cyberwarfare) is “attacks in cyberspace coordinated with military operations, which are mostly carried out by the governments of conflict states” (2016, p. 173).

Normative Regulation

In 2005, the Law on the Organisation and Competence of State Bodies in Combating High-Tech Crime was adopted in the Republic of Serbia (Narodna skupština, 2009). According to this Law on Procedures in Crimes Where Computers and Computer Systems Are the Object or Means of Execution, the Prosecutor General's Office in Belgrade is responsible for the procedure, i.e., the Special Department for Combating High-Tech Crime (2009, Articles 3 and 4). For tasks related to police competence related to high-tech crime, a special service has been established within the Internal Affairs Body to deal exclusively with high-tech crime within the Service for Combating Organised Crime (Art. 9). The department becomes active in the preliminary proceedings at the request of the specialist agency for combating high-tech crime. The main problem with this service is the lack of human resources (Bjeloš et. al., 2021, p. 97). The trial in these cases is within the jurisdiction of the Supreme Court in Belgrade, where a special department to combat high-tech crime should be established and where priority should be given to judges with special knowledge of information technology (Narodna skupština, 2009, Art. 11). In accordance with international instruments and the obligation of the Republic of Serbia to achieve international cooperation and data exchange in the field of high-tech crime, the bodies responsible for international cooperation and establishing contacts have been designated, namely the Special Prosecutor for High-Tech Crimes. Tech Crime and the Department for Suppression of High-Tech Crime (Government, 2018). In the text of the strategy to fight high-tech crime for the period 2019-2023. It is noted that taking into account the increase in these crimes along with technological development, it is necessary to improve the normative and institutional framework for combating high-tech crime, increasing the number of technological devices and establishing more effective cooperation at becomes national and international levels (2018). Among other things, the strategy states that preventive measures must be taken to raise citizens' awareness of the dangers of certain types of cybercrime. The same document notes that the Special Prosecutor's Office for Hi-Tech Crimes is a department working within the Prosecutor General's Office in Belgrade (Government, 2018). An integral part of the strategy to combat high-tech crime for the period 2019–2023. is also the action plan for the period 2019–2020. for the implementation of the strategy of aligning legislation with the legislation of the European Union in order to fight cybercrime more effectively, as well as increasing staff, staffing and creating new departments within the department (2018). In accordance with the obligation of the Republic of Serbia within the framework of the accession negotiations to the European Union – Chapter 24 (Justice, Freedom, Security) – the Republic of Serbia adopted the Convention on High-Tech Crime (Convention on Cybercrime from 2001) in 2009. The basic principle on which the Convention is based is the implementation of a common policy through the harmonisation of legislation and international cooperation (Narodna skupština, 2009). One of the examples of successful cooperation between Interpol, Europol, the FBI and our authorities is the " Armageddon" operation, launched with the aim of detecting and preventing child pornography on the Internet. The action was launched more than 10 years ago and by 2018 163 people were arrested (Interview: Branko Stamenković, Special Prosecutor for High-Tech Crimes, 2021). In order to improve international cooperation in the fight against cybercrime, the European Parliament adopted Directive 2013/40/EU (European Parliament, 2013), which lays down the rules defining cybercrime and the type and level of sanctions for these crimes. The Directive 2011/93/EU of the European Parliament on combating the sexual abuse and sexual exploitation of children and child pornography is also relevant in the field of combating cybercrime.

The Institutional Framework for Combating Cybercrime

In addition to normative regulation and its implementation, institutions are required to put the regulations into practice. In order to take measures to prevent and detect cybercrime, it is necessary to involve experts with specific knowledge in the field of cybercrime in the police and prosecutor's investigations as well as in the court proceedings (Mali et al., 2018). The chief public prosecutor's office in Belgrade is responsible for cybercrime, i.e., the special department for combating high-tech crime. For tasks falling within the jurisdiction of the police and related to high-tech crime offences, a special service dealing exclusively with high-tech crime offences has been established within the Internal Affairs Body (Narodna skupština, 2009, Art 9). Trials in these cases fall under the jurisdiction of the Supreme Court in Belgrade and in appeal proceedings under the jurisdiction of the Court of Appeal in Belgrade. Some civil society organisations, in their assessments of the Republic of Serbia's progress in Chapters 23 and 24, note that despite a good normative framework in the fight against cybercrime, results are not achieved due to insufficient human resources and their use primarily to detect criminal activities jeopardising the safety of politicians by sending threats to politicians over the Internet. The fact that the action plan for the period 2019-2020 has been adopted is cited as a disadvantage. expired without a new one being brought. Another shortcoming affecting the acting institutions is the fact that the special department for high-tech crimes at the Supreme Court in Belgrade was abolished in 2009 and since then cybercrime has been heard by judges of the Supreme and Appellate Courts in Belgrade to judge criminal cases. According to the Special Prosecutor for High-Tech Crime Branko Stamenković in an interview, the number of prosecutors, deputies and assistants in the Special Prosecutor's Office is not proportional to the number of cases processed in 2018. in 2019 there were 3,022, in 2019 3,808, in 2020 4,769 cases, and that in 2021 so far 5,135 cases have been formed" (Interview, 2021). It is a question of the special knowledge in the field of cybercrime of sitting judges. The such organisation in the courts implies that the training of judges must be from the whole criminal law and not specialised in cybercrime (Bjeloš et. al., 2021, p. 98).

Conclusion

With regard to the fight against cybercrime, normative regulations have been adopted in the Republic of Serbia, which satisfactorily regulate this area and are harmonised with the international instruments of the European Union, the number of employees in special departments and services dealing with the prevention and detection of cybercrime, and the number of offences, which is no doubt increasing every year, and we can say with certainty that such a trend will continue in the following period along with the advance of technology. The use of digital technology for the enforcement of sentences also requires the constant training of employees because the constant advances in technology also go hand in hand with the use of the same in the area of enforcement of sentences. Employees in specialised institutions fighting cybercrime must have knowledge of information technologies in order to be able to adequately respond to cybercrime, which are extremely complex crimes where it is difficult to establish the identity of the perpetrator.

In order to combat cybercrime more effectively, more attention must be paid to educating the public about the dangers of cybercrime in the near future. Education should include people of all ages and professions, from the youngest to the elderly, from businesspeople to ordinary workers, because everyone is a potential victim of cybercrime. Cybercrime is a term that encompasses a wide range of criminal activities of which all citizens are potential victims. Therefore, there is a need to start education at the earliest age and continue it into later stages of life, balancing education with greater exposure to a specific type of cybercrime at a specific age or in specific sectors.

References

Abu, A., & Israt, J. (2020). Causes of cybercrime victimization: A systematic literature review. *International Journal of Research and Review, 7*(5), 89–98. https://www.ijrrjournal.com/IJRR_Vol.7_Issue.5_May2020/IJRR0015.pdf

Bjelajac, Ž. (2021). Bezbednosna kultura kao fundamentalna ljudska potreba [Security culture as a fundamental human need]. *Kultura polisa*, *18*(1), 9–24. https://doi.org/10.51738/Kpolisa2021.18.1p.1.01

Bjelajac, Ž., & Filipović, A. (2021). Specific characteristics of digital violence and digital crime. Pravo – teorija i praksa, 38(4), 16–32. https://doi.org/10.5937/ptp2104016B

Bjelajac, Ž., & Filipović, A. (2020). Perspektive zaštite dece od zloupotreba na internetu [Perspectives of child protection from the internet misuse]. *Kultura polisa*, *17*(41), 259–271. https://kpolisa.com/index.php/kp/article/view/128/108

Bjeloš, M., Čečen, B., Elek, B., Grujičić, G., Hercigonja, S., Ignjatijević, M., Ignjatović, T., Igrutinović, M., Jovanović, M., Krunić, J., Macanović, V., Nenadić, N., Pavlović, M., Pejić Nikić, J., Petrović, P., & Teofilović, I. (2021). *PrEUgovor alarm report on the progress of Serbia in Chapters 23 and 24*. Belgrade Centre for Security Policy & Transparency Serbia.

Choi, J, Lee, S., & Dittmann, L. (2022). The Relationship between parenting practices and cyberbullying perpetration: The mediating role of moral beliefs. *International Journal of Cybersecurity Intelligence & Cybercrime*, *5*(1), 4–22. https://vc.bridgew.edu /ijcic/vol5/iss1/2

Directive 2011/93/EU on *combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA*. The European Parliament & the Council of the European Union. Official Journal of the European Union, L 335. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093

Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. The European Parliament & the Council of the European Union. *Official Journal of the European Union*, L 218/8. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32013L0040

Enjoy Safer Technology [ESET]. (2021). *European cybersecurity index: European countries with the best and worst cybersecurity*. https://www.eset.com/uk/about/newsroom/blog/european-cybersecurity-index-2021/.

Ferrara, D., Massart, P., Mc Namara, S., & Portesi, S. (2022). *2021 Report on CSIRT-LE cooperation. A study of the roles and synergies among sixteen selected EU/EEA Member states.* European Union Agency for Cybersecurity [ENISA].

Ilić, A., & Banović, B. (2021). Bezbednosna kultura mladih i savremeni rizici [Youth security culture and contemporary risks]. *Kultura polisa, 18*(1), 147–160. https://doi.org/10.51738/Kpolisa2021.18.1p.1.10

International Telecommunication Union [ITU]. (2021). Global cybersecurity index 2020 measuring commitment to cybersecurity. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Mali, P., Sodhi, J.S., Singh, T., & Bansal, S. (2018). Analysing the awareness of cyber crime and designing a relevant framework with respect to cyber warfare: an empirical study, *International Journal of Mechanical Engineering and Technology, 9*(2), 110–124. http://iaeme.com/Home/issue/IJMET?Volume=9&Issue=2

Me, G., & Pesticcio, L. (2022). Tor black markets: economics, characterization and investigation technique. In H. Jahankhani (Ed.), *Cyber criminology, advanced sciences and technologies for security applications* (119–140). Springer Nature Switzerland.

Ministarstvo unutrašnjih poslova Republike Srbije. (2021, March). *Informator o radu* [Informer on work]. http://mup.gov.rs/wps/wcm/connect/0021cb85-5d11-4cb1-ad7e-e0a124a7ab41/IOR%2Bmart%2Bcirilica2021..pdf?MOD=AJPERES&CVID=nycATmk

N1 Beograd. (2022, March 2).Nastavak akcije Armagedon: *Uhapšeno 14 osoba zbog dečje pornografije* [Continuation of the Armageddon action: 14 people were arrested for child pornography]. https://rs.n1info.com/vesti/nastavak-akcije-armagedon-uhapseno-14-osoba-zbog-decje-pornografije/

Narodna skupština Republike Srbije [Narodna skupština]. (2019). *Krivični zakonik* [Criminal Law]. (Službeni glasnik Republike Srbije, broj 85/2005, 88/2005 – ispr., 107/2005 – ispr., 72/2009, 111/2009, 121/2012, 104/ 2013, 108/2014, 94/2016 i 35/2019). Paragraf. https://www.paragraf.rs/propisi/krivicni-zakonik-2019.html

Narodna skupština Republike Srbije [Narodna skupština]. (2009a). *Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala* [*Law on the organization and competence of state bodies for the fight against high-tech crime*]. (Službeni glasnik Republike Srbije, broj 61/2005 i 104/2009). Paragraf. https://www.paragraf.rs/propisi/zakon_o_organizaciji_i_nadleznosti_drzavnih_organa_za_borbu_protiv_visokotehnoloskog_kriminala.html

Narodna skupština Republike Srbije [Narodna skupština]. (2009b). *Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu* [Law on the ratification of the Convention on high-tech crime]. (Službeni glasnik Republike Srbije, broj 19/2009). http://www.podaci.net/_z1/2129877/Z-pkvkri03v0919.html

National Crime Agency UK's. (2021). *National strategic assessment of serious and organised crime.* https://nationalcrimeagency.gov .uk/who-we-are/publications/533-national-strategic-assessment-of-serious-and-organised-crime-2021/file

Petrović, A. (2021, Decembar 27). Intervju: Branko Stamenković, posebni tužilac za visokotehnološki kriminal „Kikin zakon" ne može da se razmatra u „sajber" svetu [Interview: Branko Stamenković, special prosecutor for high-tech crime "Kika's law" cannot be considered in the "cyber" world]. *Politika*. https://www.politika.rs/sr/clanak /495574/Kikin-zakon-ne-moze-da-se-razmatra-u-sajber-svetu

Pournouri, S., Zargari, Sh., & Akhgar, B. (2022). Predicting the cyber attackers; A comparison of different classification techniques. In Ha. Jahankhani (Ed.), *Cyber criminology, advanced sciences and technologies for security applications* (pp. 169–181). Springer Nature Switzerland.

Stojšić Dabetić, J. (2020). Moderni i postmoderni koncept detinjstva u svetlu osiguranja bezbednosti dece u digitalnom društvu [Modern and postmodern concept of childhood in the light of ensuring child safety in digital society]. *Kultura polisa, 18*(1), 161–173. https://doi.org/10.51738/Kpolisa2021.18.1p.1.11

Sabillon, R., Cano, J, Cavaller, V., & Serra, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security*, *4*(6), 165–176. www.ijcncs.org

Sallavaci, O. (2022). Crime and social media: Legal responses to offensive online communications and abuse. In H. Jahankhani (Ed.), *Cyber criminology, advanced sciences and technologies for security applications* (pp. 3–23). Springer Nature Switzerland.

Top Business Tech Events [TBTECH]. (2021, July 11). Which European countries have the best and worst cybersecurity? https://tbtech.co/news/which-european-countries-have-the-best-and-worst-cybersecurity/

Stamenković, B., Živanović, S., Paunović, B., & Stevanović, I. (2017). *Vodič za sudije i tužioce na temu visokotehnološkog kriminala i zaštite maloletnih lica u Republicu Srbiji* [Guide for judges and prosecutors on the topic of high-tech crime and the protection of minors in the Republic of Serbia]. Save the Children in North West Balkans, Sarajevo.

Vlada Republike Srbije [Vlada]. (2018). *Strategija za borbu protiv visokotehnološkog kriminala za period 2019–2023. godine* [Strategy for the fight against high-tech crime for the period 2019-2023]. (*Službeni glasnik RS, broj 71*). http://www.pravno-informacionisistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2018/71/1/reg

Sajber kriminal u Republici Srbiji: prevalenca, stanje i perspektive

Lazar V. Stošić
Don državni tehnički univerzitet, Rostov na Donu, Rusija
Aleksandra V. Janković
Akademija strukovnih studija Južna Srbija – Leskovac, Odsek
Visoka škola za vaspitače Bujanovac

Sažetak

Slučajevi anonimnih dojava putem računara o postavljenim bombama u školama i drugim važnim ustanovama širom Srbije obeležili su 2022. godinu. Ovi događaji pokrenuli su debatu u javnosti da li organi zaduženi za borbu protiv sajber kriminala mogu adekvatno da odgovore na takve napade. Sve je veći broj korisnika interneta, a samim tim i potencijalnih žrtava sajber kriminala, kao i obaveze država da zaštite građane. Poslednji događaji pokazali su stepen ranjivosti i rizike po društvo koje donosi visokotehnološki kriminalitet. U radu se analizira normativni i institucionalni okvir borbe protiv sajber kriminala, i podaci Ministarstva unutrašnjih poslova o sajber kriminalu. Cilj rada je da se na osnovu analize postojeće zakonske regulative sajber kriminala i analize institucionalnog okvira kod nas i u pojedinim zemljama Evrope daju predlozi za eventualne izmene, a kako bi se obezbedila efikasnija zaštita od sajber kriminala. U radu je primenjen normativni metod kao i komparativni metod za prikaz mera koje se preduzimaju u drugim zemljama. Za analizu prikupljenih podataka korišćena je deskriptivna analiza. Zaključak je da i pored dobrog normativnog okvira borba protiv sajber kriminala nije adekvatna pre svega zbog broja ljudi koji rade u specijalnim odeljenjima i odsecima u tužilaštvu i policiji, a koji je daleko manji u odnosu na broj dela koji se dešava, a koji iz godine u godinu raste. Opasnost predstavlja i nedostatak svesti kod većeg broja ljudi o opasnostima korišćenja interneta, zbog čega bi u narednom periodu više pažnje trebalo posvetiti edukaciji građana. svih uzrasta o opasnostima i vrstama sajber krivičnih dela.

Ključne reči: sajber kriminal, krivična dela, institucije, normativna regulativa, informacione tehnologije