Bjelajac Željko*
https://orcid.org/0000-0003-4953-8779
Filipović M. Aleksandar**
https://orcid.org/0000-0002-1097-2079

UDK: 316.624:004.738.5
Original scientific paper
DOI: 10.5937/ptp2104016B
Received: 10.11.2021.
Approved on: 19.12.2021.
Pages: 16–32

SPECIFIC CHARACTERISTICS OF DIGITAL VIOLENCE AND DIGITAL CRIME

ABSTRACT: Migration of many aspects of human life and work into the online sphere has become an integral part of everyday life and it is difficult to imagine the functioning of any aspect of life without the Internet and the space in which most human interactions take place. One such large and significant new form has created a large number of smaller ones, and conditioned the transformation of things and phenomena from the physical world into completely new digital forms. The same happened with violence, as a phenomenon, a pattern of behavior and a part of human nature from the very beginnings of civilization, which took its new form being called a digital violence. It does not necessarily have to be online, but it is necessarily related to digital devices. To the problem of digital crime there should be added a digital violence as a contemporary problem, especially when we talk about legal regulatory mechanisms, although these two phenomena, with frequent overlaps, do not necessarily have to be contained in each other, but they are equally important.

Online and offline digital spaces represent just a new field in which violence and crimes are committed, but the virtual characteristic of these spaces is only an additional specific feature, because their consequences are felt in the physical, real world, and in that sense, the border between virtual and real is invisible. This paper aims to explore the ontological determinants of violence and digital violence, to identify specific forms of digital violence

* LLD, Full professor, The Faculty of Law for Commerce and Judiciary, The University of Business Academy, Novi Sad, Serbia, e-mail: zdjbjelajac@gmail.com
** PhD, Assistant Professor, The Faculty of Economics and Engineering Management, The University of Business Academy, Novi Sad, Serbia, e-mail: sasha.filipovic@gmail.com

and digital crime, as well as to analyze existing regulations aimed at combating digital violence and digital crime.

Keywords: *violence, digital violence, digital crime, legal regulations*

1. Introduction

The technological development of modern society has led to the multiplication of the space in which social life and social interactions take place. If we say that technological development has brought a new space for social interactions, we would significantly reduce the real situation, because it is not a new space, but an incalculable number of new spaces, which can be classified as Internet spaces, but as the Internet is only a means by which these spaces are approached, such a claim is not precise enough. It can be said that modern society is a society of countless illuminated screens. These screens are not just a two-dimensional representation of traditional media content, on the contrary – they are the means by which the greatest interconnection of people and content is achieved. Digitalization have brought unprecedented changes, and not only in the technological sense. The digital revolution has embraced all segments of society and changed the way human beings function even on a daily basis, from socialization to business, encompassing most things in between (Bjelajac & Filipović, 2021). Of course, as most of his life migrated to online digital spaces, it is understood that violence and crime, as an inseparable part of human nature and behavior, also migrated, and with that migration they acquired a new form and characteristics, while retaining most of their physical characteristics. But it is precisely these new forms and features that create a great challenge, both in the theoretical and in the practical sense. A rare thing in which there is no difference between the physical and the digital, when we talk about violence and crime, are the consequences, which are the same regardless of the space and the means by which the violence is committed. This paper starts from several hypotheses: that due to the ontological nature of violence, and thus digital violence and crime, it is not possible to completely suppress them; that the difference between violence in the real world and violence in the digital world is invisible, because the consequences and pain caused by digital violence are also felt in the real world; and that analogous to the regulation, suppression and control of violence and crime committed in the physical world, there must be regulation, suppression and control of violence and crime in the digital world, taking into account all the specifics and differences between the physical and digital. The aims of the

paper are to investigate the phenomenological and ontological determinants of violence and digital violence, the differences between violence in the digital world and violence in the real world, to identify specific forms of violence and crime in the digital world and to analyze existing regulations to control and combat digital violence and crime.

2. On the ontological nature of violence and digital violence

Digital violence has its ontological root and origin in violence in general, so that digital violence in its being differs little or not at all from general violence as a necessary essential feature of members of the human species. The presence of different types of violence makes it difficult to identify its general characteristics, but all chances are that "violence is a manifestation of the very structure of being " (Денисов, 2008). Violence is a specific form of relationship whose use is associated with "use of force", "infliction of physical, spiritual and property damage", "violation of one's interests and rights", "suppression of free will". Violence or the threat of its use forces people to behave inappropriately to their desires, hinders the "somatic and spiritual realization of human potential" (Денисов, 2008).

World Health Organization has defined violence as "the intentional use of physical force or power, threatening or actual, against oneself, another person, or against a group or community, which results in or has a high probability of injury, death, psychological injury, malformation, or poverty. This definition includes the very intention to commit the act, regardless of the outcome it creates. However, in general, anything that leads to harm or injury can be described as violence even though it was not planned as an act of violence (by or against a person) (World Health Organization n.d). In the essence of the being of violence, there are two firmly rooted phenomena – the intention to commit violence and the primary evil in man as the spiritus movens of violence, a noumenon that always means pain for the victim of violence.

In philosophical interpretations of the nature of human violence, as presented by Plato (2013) and later, among others, Hume (1896), Hobbes (2004) and Russell (1949), violence is highly ranked in the primary series of human instincts, moreover, there is a constant that indicates that human nature is ontologically intrinsic to violence, which, according to this thesis, is not only the most effective, but often the only means by which man can fulfill his desires. some can be vital to the life and survival of the individual, family, group, and even the state. These desires and the effort of man to realize them represent the primary initiator of violence, which in that context is by no means evil, is

not harmful and represents a praiseworthy activity. While we tend to declare such a view savage and erroneous, placing the habit of "doing evil for evil and violence for violence" in the wild past measured by millennia, it is not so. Haven't we, in the immediate past and the immediate environment, had armed conflicts and the ones most celebrated were precisely the people and groups that committed the greatest violence. Even today, many individuals and large parts of society worship them, and their activities are declared historically and existentially useful works.

In Leviathan (1651), Hobbes claims that the human person is ontologically destined to act according to natural law, that is, according to the freedom that is given to every human being by birth and being on Earth. This freedom that nature gives to man makes every man have the right to make his own decisions about how to use his own power to preserve his own nature and his life, and consequently man has the freedom to do whatever he thinks is the most appropriate means to do so (Hobbes, 2004, pp. 72–93). Hobbes claims that all people are equal in this and that they all believe in themselves equally, so their equal status encourages equality in their minds to realize their desires. The result is that where two or more people want what not everyone can have at the same time, they necessarily become enemies and necessarily commit violence. This point is clearly stated in the quote that "the condition of man is a condition of war of everyone against everyone, so that everyone rules with his reason and can use everything he likes that could help him save his life from the enemy" (Hobbes, 2004, p. 90). Life, according to Hobbes, is a selfish quest to saturate desires, and to that end people will seek to destroy and subjugate each other (see more: Shitta-Bey 2016).

At the international conference that was held in Russia in 2018 under the name "*Насилие в цифровую епоху*" (Violence in the digital era), an interesting paper "Ontological ultimatum and the nature of violence" was submitted, in which the author starts from the thesis that aggression and human violence, and even doing evil to others is not a matter of his choice, but it is natural impulses deeply ingrained in the ontological being of man that make aggression, violence and evil a way of life and a way of expressing natural instincts that society cannot suppress forever (Оболкина 2018). At the same time, "aggression and human violence, as well as doing harm to others" in the sense of this work, were if not the only, then the best way to succeed in life, to gain much-needed fame and to live to a decent old age.

Bertrand Russell wrote: "We have all kinds of aggressive impulses, which society forbids us to follow. I think that ordinary people cannot be happy without competition, because competition has been, since the beginning of man, the

inspiration for most serious activities. So, one should not try to abolish the competition, but one should try to practice it in forms that are not too dangerous. The primitive competition consisted of who would be the first to slaughter his rival, his wife and children; modern competition in the form of war still boils down to that. Anyone who hopes that wars will be eradicated in time should seriously consider the problem of safely satisfying the instincts we inherited from numerous generations of our wild ancestors. Many people are happier in war than in peace, provided they do not suffer much on their own. A quiet life can be boring. The monotonous existence of an exemplary citizen, preoccupied with making ends meet in a humble capacity, leaves completely unsatisfied that part of his nature which, had he lived 400,000 years ago, would have been completely filled with the search for food, beheading enemies and fleeing tigers" (Russell, 1949). This view is also articulated by Tofler when he observes that power is a reciprocal desire, and that human desires are infinitely different. Anything that can fulfill someone's desire is a source of power (Tofler, 1990).

3. Digital violence and digital crime

Like the majority of terms belonging to the sphere of the information and communications technologies, digital violence is a relatively new phenomenon which becomes a topic of serious scientific discussions in recent decades. There is a number of definitions of digital violence, and some are more general and include all forms of disturbance by using digital technologies, while the others are focused on specific forms of digital violence (Filipović & Vojnić, 2019). Nonetheless, the most important thing is mutual to violence in physical world and digital violence, that consequences are felt in physical world, and the space where the violence happens in merely a new and different challenge. A specific and particularly harmful form of both violence and crime in digital space is Internet pedophilia. Pedophiles use the Internet in various ways, whether to connect with children, make friendships, organize live meetings, or as a means to find, keep, and distribute child pornography. The Internet is also used as a means for interconnecting in pedophile networks, where they share experiences, advice, and visual content. Still, the Internet is not usable to pedophiles only because of the easy access to children, their identity, and child pornography. The internet is an ideal tool for pedophiles as it offers them complete safety and absolute anonymity (Bjelajac & Filipović, 2020). And in the case of Internet pedophilia and other migrated forms of violence and crime, the difference between digital and physical, if we look at the problem from the victimological perspective, is almost invisible.

As much as the differences between violence and digital violence were academic, the difference between general crime and digital crime is so great that countering digital crime with methods developed for general crime is almost impossible. When we consider digital crime as a group of practical actions that individuals or groups of people undertake, the first problem is the terminological definition of the term. Is it digital crime, cybercrime, high-tech crime, or something fourth. All the definitions are similar, but they are by no means the same, and when we start the meticulous scientific treatment, we very quickly notice the crucial differences.

The problems of preventing cybercrime were first discussed at the Eighth United Nations Congress in Havana in 1990. Since then, the UN has been actively considering various aspects related to the use of computers. In 1992, the OECD prepared the "Information Systems Security Directives". They were subsequently revised and adopted on 25 July 2002 as a Recommendation of the OECD Council as a "Directive on the Security of Information Systems and Networks: Building a Security Culture" (Organisation for Economic Co-operation and Development, 2003).

It seems that the crucial problem is that criminological science, followed by practice, has completely unprepared for the escalation of "new" digital crimes. The operatives who were engaged in detecting crime in the field found themselves in a territory they do not know. The courts could not conduct proceedings because many of the crimes that caused great harm to society and individuals were not codified as crimes at all. The state of criminological theory and practice, which in many countries suddenly began to understand what it was about, required a significant reorientation of activities, primarily law enforcement services, to actually ensure criminological security of individuals, society and the state in the context of digitalization. Fulfillment of this task required and still requires serious training of experts who must be able to investigate the current state of crime in the development and use of digital technologies, identify the features of the cause-and-effect complex, analyze the socio-demographic and moral-psychological characteristics of the criminal who has committed a crime in the field of digital technologies, to determine the main directions of confrontation with new types of crimes. Only criminology as a social-legal general theoretical and applied science and discipline can provide the necessary knowledge for that. It is called to investigate crime as a social phenomenon, to determine the essence and forms of its manifestation, to identify patterns of occurrence, existence and change of crime (Ищук, Я. Г., Пинкевич, Я. Г., & Смольянинов, Е. С., 2021).

Serebrennikova wrote about some interesting ideas about the correlation of digital technology and new criminological science: "The structure of digital technology is of crucial criminological importance for the detection, investigation and investigation of crimes. The first factor in the structure is large databases (Big Data) with network access. Other are computational capabilities, expert systems, and artificial intelligence, and to some extent modeling as part of the psychophysiological and mental process. Third, it is cloud technology (storage and computing) as well as distributed computing. Here we talk about a fairly wide range of modeling methods, correlation, structure of contingency tables, performing discriminant, regressive, variational, factorial and other types of analysis, application of seasonal fluctuation methods, probability limitation (including least squares method), as well as calculation methods growth using the index of average annual rates. Digital criminology is seen as a set of more advanced technological plans – methods that are developed on the basis of mathematical prediction. It is a computerized processing of quantitative and qualitative parameters of crime and mathematical identification of different types of dependence (on time, place and other variables). Mathematical processing of criminological information is rightly given great importance, which indicates new possibilities for specifying predictions. At the same time, it would be irrational to reduce digital criminology to just that, even if it is a rapidly evolving technological component, since, in essence, there is a danger of neglecting criminological theory. It is obvious that the development of technology, even the most advanced, does not in itself constitute a perfect methodological basis for criminological research. The development of technology without the support of theory does not identify enough potential directions for improving the theory of crime prevention, taking into account its current state" (Serebrennikova, 2020).

It is similar with the definition of digital crime. A significant factor that complicates the definition of digital crime is the primary legal dilemma, as this term is understood and defined differently in different countries. There is the experience of scientists in the study of cybercrime, but the postulates of that experience do not give a complete picture and definition of crimes committed in the field of digital technologies. It is known that the term "computer crime" was first used in one of the reports of the Stanford Research Institute (1999). Later, articles on cybercrime adopted the following classification according to which a computer can be: a subject of crime; may be the subject of a crime; and can be a tool. There was a fourth option, proposed in 1973 – the computer as a symbol, but that option was abandoned during the 1980s (Ищук, et al., 2021).

Over time, two primary definitions of cybercrime in a narrower and broader sense have been developed. In the first case, cyber crime is considered to be any illegal behavior in the field of electronic transactions that aims to violate the security of computer systems and the data they process. In a broader sense, crime is considered to be any illegal behavior committed through a computer network or through computer systems. As the case law proves, this should include the illegal possession, supply or dissemination of information via a computer system or network.

The definition of cybercrime was given in 2000 at the session of the Tenth UN Congress on Crime Prevention and Criminal Justice. It has been established that a computer crime refers to any criminal offense that can be committed through a computer system or network, within a computer system or network, or against a computer system or network. In principle, it covers any crime that can be committed in an electronic environment. But already in the framework of the Eleventh UN Congress on Crime Prevention and Criminal Justice, 2005, it was proposed "that this conceptual model be formulated differently, taking into account crimes related to the use of computers as prohibited by law and / or case law, which is: a) focused on the computer sphere and communication technologies; b) involves the use of digital technology in the commission of a criminal offense; c) involves the use of computers as tools in the process of committing other criminal offenses, and, accordingly, the computer acts as a source of electronic procedural evidence" (Computer Crime Research Center 2005).

We mentioned Stanford University, whose research teams have been dealing with all aspects of what we call computer crime in this paper for decades. We also recommend their thoughts on defining this type of crime and determining their elements (Stanford Research Institute, 1999).

The computer crime literature focuses on computer-related scams. "Fraud is the intentional or deliberate distortion of the truth in order to gain an unfair advantage" (Strothcamp, 1999). This is certainly a big part of computer crime, but it may be a little too narrow for our needs. Many others, when they think of computer crime, think only of those who break into computers to steal or destroy information.

We can get a slightly broader definition by studying what law enforcement agencies are actually researching. The FBI's National Computer Crime Squad (NCCS) deals with all crimes involving computers in two or more states. The following are considered important computer crimes:

- Intrusions into the public switched network (telephone company)
- Larger intrusions into the computer network

- Violation of network integrity
- Privacy breach
- Industrial espionage
- Pirated computer software
- Other crimes in which the computer is the main factor in the commission of a crime.

The Jones Telecommunications & Multimedia Encyclopedia states: "Some issues are carefully studied by everyone, from network veterans and law enforcement agencies to radical experts, including:

- Intrusion into a computer network
- Industrial espionage
- Software piracy
- Child pornography
- Email bombing
- Password finders
- Forgery
- Credit card fraud."

These lists are useful for thinking about areas of computer crime, but a reasonably concise definition comes from the end of the NCCS list: "crimes in which the computer is a major factor in the commission of a crime." This definition may be a little vague, so it might be useful to reduce it to crimes in which the computer is the primary, not just the main factor. Any real-world definition is necessarily somewhat arbitrary, but this working definition will be helpful in thinking about what we consider cybercrime" (Stanford Research Center, 1999).

4. Legal regulation of digital violence and digital crime

We live in an era of scientific and technological development, to unprecedented proportions. Along with the improvement, it has become increasingly common for technologies to be used for harassment and abuse. Digital abuse can occur in people of all ages, although it is especially common among teenagers and young people who use smartphones more often. Signs of digital abuse may include, but are not limited to: intimidation and harassment, surveillance and stalking, sexual coercion, possession and control. The specifics of digital violence are reflected in the fact that they include all cases in which someone uses electronic devices (mobile phone, computer, camera…) and

the Internet to tendentiously frighten, insult, humiliate or otherwise injure someone.

The life and activities of children in the modern age, in a significant part, take place in a digital environment, most often in spending time on the Internet. Learning, research, mutual communication with family and friends, takes place through digital devices that represent the focus of attention, wishes and desires of every child today. All this leads to an increased interest of children in exploring that boundless space of information and content, and on that path of search, they often face problems. The biggest of them is the whirlpool of digital violence, which they fall into recklessly, very easily, and the way out is difficult to find, most often by accident and after a hard fight with oneself, one's own environment and the aggressor or more of them (Mirković, 2019). Therefore, it is an incoherent and deceptive notion that digital violence takes place somewhere in the "virtual" world and is therefore less dangerous than the classic violence that takes place in the real world.

International conventions, resolutions and directives adopted at the level of the United Nations, the Council of Europe and the European Union, states and legally oblige states to establish a comprehensive legislative framework aimed at preventing abuse and violence against children in the digital environment, timely detection of such behavior, prosecution of perpetrators, as well as to take all necessary actions to provide assistance and support to child victims, to raise citizens' awareness of the unacceptability of any form of abuse and exploitation of a child, including that committed through information and communication technologies. This includes the obligation of the state to take all necessary legislative, administrative, social and educational measures, extraterritoriality or cross-border prosecution and conviction of perpetrators, as well as an adequate and concrete definition of criminal activities through information and communication technologies that harm children (child sexual abuse, recruitment, persuasion and encouraging children to do harmful activities, etc.), the best interests of children, transparent information on the risks of using such technologies and means of protection against exploitation (Ivanović, 2019). With this in mind, the protection of young people from online abuse and exploitation is guaranteed by numerous international and national documents, in order to provide support and a framework for measures to protect children from all forms of violence, exploitation and abuse in the digital environment. Despite everything, there is a huge gap between the potential of the normative and the real. For example, Serbia has ratified numerous conventions, protocols, guidelines for respecting, protecting and exercising the rights of the child in the digital environment. In addition to

the provisions of the Constitution, the Criminal Code, strategic documents, other relevant protocols and legal acts have been adopted, which form, among other things, a unique and comprehensive legal framework, including Law on the Fundamentals of the Education System, Rulebook on the protocol of actions in response to violence, abuse and neglect, Special Protocol for the Protection of Children and Students from Violence, Abuse and Neglect in Educational Institutions, and Framework action plan for the prevention of violence in educational institutions. Unfortunately, as in many social spheres, it has been shown that the volume of documents in this domain cannot cover anomalies, which are becoming more and more frequent, which indicates a serious gap between law and justice. The obvious and sightless violation of regulations related to the digital environment and the media space in general, where immorality and violence are openly promoted, confirms that the difference between normative and real is growing in this area and that what is in the regulations is not in line with reality.

As for our country, Serbia is trying to be technologically developed. In systemic activities towards high-tech crime, Serbia, according to state services, is in the upper half of the world. Data from independent screenings indicate slightly worse ratings (Beogradski centar za bezbednosnu politiku 2016).

"In the process of Serbia's accession to the European Union, cyber security and high-tech crime are subject to regulatory harmonization within Chapter 24 – Justice, Freedom and Security. The European Commission's Chapter 24 screening report points to the fact that the fight against high-tech crime in Serbia is still in its infancy. According to the index of development and use of information and communication technologies of the UN International Telecommunication Union, Serbia is a medium-developed country with a tendency to decline. Serbia also records a significantly lower rate of Internet representation in households (66.2%) than the average of the European Union countries (79.3%). From the formal legal point of view, Serbia is not in a bad position, since as a candidate for EU membership, it follows the legal guidelines from Brussels. Although the practice can be discouraging, the fact that the current laws of Serbia are largely harmonized with global, and especially European standards for the fight against cybercrime, which is a necessary condition for institutional improvement of the practice, is extremely important" (Beogradski centar za bezbednosnu politiku 2016).

For Serbia, as for a large number of European countries, it is characteristic that almost all forms of high-tech (computer) crime appear. Piracy is the most widespread, but there are also computer sabotages, frauds, misuse of payment cards, unauthorized use of data, pedophilia, etc. Computer crimes were

introduced by the Criminal Code of Serbia from 1998, when certain crimes were identified as "crimes against computer data". In a separate section, the Criminal Code defines the terms used in the law, and within that provides legal definitions relating to computer crimes. The basic terms are: computer data, computer network, computer program, computer virus, document, movable item.

The Law on the Organization and Competence of State Bodies for the Fight against High-Tech Crime entered into force on July 26, 2005, in response to high-tech crime, and "regulates the education, organization, competence and powers of special organizational units of state bodies for detection. criminal prosecution and trial for criminal offenses determined by this law". In addition to defining what high-tech crime is and the scope of this law, the District Public Prosecutor's Office in Belgrade for the territory of the Republic of Serbia has been appointed to act in criminal cases of this law, and a special department for fighting high-tech crime is being organized within it. The work of this department is managed by a special prosecutor appointed by the Republic Public Prosecutor, with priority given to public prosecutors and deputy public prosecutors who have knowledge in the field of information technology. The special prosecutor is appointed for four years with the possibility of re-election.

5. Discussion

The history of great technological discoveries has shown that the most significant technological discoveries very quickly end up in the hands of criminals and help them carry out illegal activities. Only later do technological discoveries become useful for the rest of humanity. It is the same with information and communication technologies (ICT). The development of ICT and related technologies has raised to a new and higher level the task of combating crimes committed through their use and minimizing the damage caused by these crimes. The growth in the volume of new types of crime alarmed society and the government at the moment when, with the help of ICT and computer fraud, huge amounts of money began to flow into the accounts and pockets of criminals. Criminologists are also alarmed, since the penetration of criminals into the virtual environment and their mastery of new technologies has taken on threatening dimensions, introduced a new criminal motivation, but at the same time, to some extent, encouraged the development of information and telecommunications technologies.

Some authors (Serebrennikova, 2020) believe that combating and combating digital crime requires a critical re-examination of existing criminological

methods and an attempt to go beyond the known, "generally accepted" ways of working in neoclassical criminology. The development of the concept of digital criminology cannot be reduced only to a set of technologically advanced methods that are developed on the basis of mathematical prediction, ie. computer processing of quantitative and qualitative parameters of crime, mathematical identification of different types of dependence. The modern information – analytical sphere of law enforcement activities includes the use of digital criminological tools in crime prevention programs, mathematical methods of crime analysis, profiling, etc. Their totality is mainly applicable for criminological analyzes and forecasts, but there is no necessary theoretical basis that corresponds to the tasks of fighting crime in the digital world, which is still being formed on the basis of digital criminology, criminological neoclassicism, overall scientific achievements about society and man. Forecasts for the next industrial revolutions predict a sharp acceleration of the pace of technology development, systemic transformation of production and management, which will not only push the global growth of living standards, but also increase inequality, and therefore give rise to crime. It is these aspects that must be taken into account when predicting the further scientific development of digital criminology, whose theories should be based on conceptual models of social development in the near future. The social consequences of the predicted new industrial revolutions will inevitably become common determinants of future crime, as they have always been in the past.

In that sense, digital criminology emphasizes the interdisciplinary integration of scientists who represent the complex of sciences of the so-called criminal cycle. The literature also discusses the need, and even the necessity, for the return of criminology to a holistic, traditional picture of the world, which will be quickly filled with new knowledge in accordance with the development of the information society. In this case, a special role will belong to the new, digital criminology, within the framework and means in which legal, humanitarian and natural-elementary knowledge will converge. Within traditional criminology, the problems of the criminal's identity have, at first glance, been solved and comprehensively investigated, which, however, cannot be said of a "digital" criminal operating in a virtual, seemingly invisible world. In that sense, the criminological literature on the problems of the development of the criminal personality is still mostly "analog", and does not take into account the specifics of the development of the digital society. The criminology of most countries is still dominated by a mechanical, traditional and somewhat simplified view of the personality of the criminal, who, as a rule, depersonalizes.

6. Conclusion

The digital world has led to new variability in the development of the situation, since the circumstances that can lead to digital crime can develop in both the real and virtual world. Crimes committed on the basis of and under the influence of computer games, communication on social networks, various forms of internet fraud require criminological analysis. Scientists are increasingly pointing out the discrepancy between old, traditional forms and methods of investigating information and "new" crimes with new illegal manifestations in the digital sphere or with the use of the digital sphere of life. In that sense, the imperative is to "return" the identity of criminals to the focus of criminological research. It is necessary to accept the emergence of "new" crimes that carry the specifics of the information age, the number of which will most likely only increase and worsen in the future. The forecast of the effectiveness of measures to combat such crime is generally pessimistic. The forecasts of the so-called fourth industrial revolution indicate a sharp acceleration of the pace of technology development and a systemic transformation of production and management. The social consequences of the projected new industrial revolutions will inevitably become the general determinants of the crimes of the future, as they have always been in the past.

Bjelajac Željko
Redovni profesor, Pravni fakultet za privredu i pravosuđe, Univerzitet Privredna akademija, Novi Sad, Srbija

Filipović M. Aleksandar
Docent, Fakultet za ekonomiju i inženjerski menadžment, Univerzitet Privredna akademija, Novi Sad, Srbija

SPECIFIČNOSTI DIGITALNOG NASILJA I DIGITALNOG KRIMINALA

REZIME: Migracija brojnih aspekata ljudskog života i privređivanja u onlajn sfere postala je neodvojivi deo svakodnevice i teško je zamisliti funkcionisanje bilo kog aspekta života bez interneta i prostora u kome se odvija

najveći deo ljudskih interakcija a koji on omogućava. Jedna tako velika i značajna nova forma stvorila je veliki broj manjih, i uslovila transformaciju stvari i fenomena iz fizičkog sveta u sasvim nove digitalne forme. Isto se desilo i sa nasiljem, kao fenomenom, obrascem ponašanja i delom ljudske prirode od prapočetaka civilizacije, koje je dobilo svoju novu formu koju generalno zovemo digitalnim nasiljem, a koje ne mora nužno da bude onlajn, ali je nužno vezano za digitalne uređaje. Digitalnom nasilju kao savremenom problemu treba dodati i problem digitalnog kriminala, naročito kada govorimo o pravnim regulativnim mehanizmima, iako ta dva fenomena, uz česta preklapanja, ne moraju nužno da se sadrže jedan u drugom, ali su podjednako važna. Onlajn i oflajn digitalni prostori su samo novo polje u kome se vrše nasilje i krivična dela, ali virtuelnost tih prostora predstavlja samo dodatnu specifičnost, jer se njihove posledice osećaju u fizičkom, realnom svetu, i u tom smislu, granica između virtuelnog i stvarnog je nevidljiva. Ovaj rad ima za cilj da istraži ontološke odrednice nasilja i digitalnog nasilja, da identifikuje specifične oblike digitalnog nasilja i digitalnog kriminala, kao i da analizira postojeću regulativu namenjenu suzbijanju digitalnog nasilja i digitalnog kriminala.

***Ključne reči*:** *nasilje, digitalno nasilje, digitalni kriminal, pravna regulativa.*

References

1. Beogradski centar za bezbednosnu politiku (2016). *Sajber kriminal u Srbiji pred otvaranje poglavlja 24,* [*Cyber criminal in Republic Serbia before opening chapter 24*]. Downloaded 2021, August, 10 from https://bezbednost.org/publikacija/sajber-kriminal-u-srbiji-pred-otvaranje-poglavlja-24
2. Computer Crime Research Center (2005). Preliminary results of the Eleventh United Nations Congress on Crime Prevention and Criminal Justice in Bangkok, April 2005, Downloaded 2021, August, 11 from http://www.crime-research.ru/analytics/crime_bangkok
3. Hobbes, T. (2004). *Levijatan ili građa, oblik i moć crkvene i građanske države* [*Leviathan or material, form and power of the church and civil state*]. Zagreb: Jesenski i Turk
4. Hume D. (1896). *A Treatise of Human Nature*. Oxford: Clarendon Press
5. Ivanović, J. (2019). *Smernica za profesionalce u zaštiti dece od digitalnog nasilja u Republici Srbiji* [*Guidelines for professionals in child protection from digital violence in the Republic of Serbia*]. Beograd: Save the Children in North West Balkans

6. Mirković, A. (2019). *Najbolje prakse podrške deci žrtvama nasilja u digitalnom okruženju* [*Best practices of support of child victims of violence in digital environment*]. Beograd: Save the Children in North West Balkans
7. Organisation for Economic Co-operation and Development. (2003). *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, Downloaded 2021, August, 14 from https://www.oecd.org/sti/ieconomy/15582276.pdf
8. Platon (2013). *Država* [*The Republic*]. Beograd: Dereta
9. Russell, B. (1949). *Authority and the Individual.* London: George Allen and Unwin
10. Serebrennikova, A. V. (2020). Criminological problems of the digital world (digital criminology), *Russian Journal of Criminology*, *14* (3), pp. 423–430
11. Shitta-Bey, O. A. (2016). A Discourse on the Ontology of Violence, *Kaygi: Uludağ Üniversitesi Fen-Edebiyat Fakültesi Felsefe Dergisi* (27), pp. 151–166
12. Stanford Research Institute (1999). Computer Crime; The Wave of the Future, Downloaded 2021, August, 14 from https://cs.stanford.edu/people/eroberts/cs181/projects/computer-crime/definition.html
13. Strategija za prevenciju i zaštitu dece od nasilja za period od 2020. do 2023. godine [Strategy for prevention and protection of children from violence 2020-2023], *Službeni glasnik RS*, br. 80/20
14. Strothcamp, D. (1999). Fraud and Computer Crime*, Cleveland State University,* Downloaded 2021, August, 16 from http://www.csuohio.edu/accounts/Strothcamp/TOPIC07/sld001.htm
15. Toffler, A. (1990). *Power shift: Knowledge, Wealth, and Violence at the Edge of the 21st Century*. New York: Bantam Books.
16. World Health Organization, (n.d), Violence prevention, Downloaded 2021, August, 11 from https://www.who.int/violenceprevention/approach/definition/en
17. Bjelajac, Ž, & Filipović, A. (2020). Internet i društvene mreže kao neograničeni prostor za koncentraciju i multiplicirano prisustvo pedofila [The Internet and social networks as unlimited space for concentration and multiplied presence of pedophiles], *Kultura polisa, 17* special edition, pp. 29–40
18. Bjelajac, Ž. i Filipović, A. (2021). Fleksibilnost digitalnih medija za manipulativno delovanje seksualnih predatora [Flexibility of digital media for manipulative activities of sexual predators], *Kultura polisa, 18* (44), pp. 51–67

19. Denisов, В. В. (2008). Философия насилия [Philosophy of violence], *Философия и общество,* (1)*,* pp. 39–56
20. Ищук, Я. Г., Пинкевич, Я. Г., & Смольянинов, Е. С. (2021). *Цифровая криминология* [*Digital Criminology*]. Москва: Академия управления МВД России
21. Krivični zakonik Republike Srbije [Criminal Code of the Republic of Serbia], *Službeni glasnik RS,* br. 85/05, 88/05 – ispr., 107/05 – ispr., 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 i 35/19
22. Оболкина, С. В. (2018). *Онтологическая ультимативность и природа насилия* [*Ontological ultimatum and the nature of violence*]. Violence in the Digital Age Conference, Tyumen, Russia
23. Strategija razvoja informacione bezbednosti u Republici Srbiji [Development strategy of information security in the Republic of Serbia]. *Službeni glasnik RS*, br. 53/17
24. Ustav Republike Srbije [Constitution of the Republic of Serbia]. *Službeni glasnik RS*, br. 98/06
25. Filipović, A. & Vojnić, S. (2019). Bezbednosni izazovi na internetu kao novom prostoru za vršenje nasilja [Internet as a new space for perpetrating violence and its security challenges], *Kultura polisa*, *16* (39), pp. 263–273